

CHAPTER 4

AIS SECURITY

LEARNING OBJECTIVES

Upon completing this chapter, you should be able to do the following:

- *Identify the procedures for issuing and updating user identification and passwords and for validating customer authorization.*
 - *Identify the procedures for performing, directing, and validating security inspections and for reporting and investigating security violations.*
 - *Identify the procedures for developing and updating security plans.*
 - *Recognize how to implement and evaluate countermeasures and contingency plans.*
 - *Identify the procedures for preparing and updating emergency action plans.*
 - *Explain how to implement and evaluate security test and evaluation procedures.*
 - *Explain how to safeguard AIS classified material.*
-

AIS security is a cycle of events that never ends. You start with the development of a security plan for the facility. This plan includes conducting an in-depth risk assessment covering different types of disasters that threaten the security of the AIS facility. Once the security plan is in place, the inspections begin. You will be responsible for preparing the inspection plan and conducting the inspection using the guidelines provided in the security instructions.

In this chapter, you will learn about AIS security—from the implementation of the security plan through conducting security inspections. This includes AIS threat and risk analysis, disaster protection, contingency planning, inspection preparation, and data privacy.

WHAT IS AIS SECURITY?

AIS security is more than protecting classified information and keeping unauthorized personnel out of

your AIS facility. It is protecting equipment, media, data and people. AIS security is limiting access, avoiding misuse, and preventing destruction. It is preventing changes to data that would make the data unreliable. It covers the denial of service and the destruction of computer rooms, the loss of confidentiality, fraud, the theft of computer time as well as the computer itself. AIS security is a critical part of your job.

As you probably noticed from reading the learning objectives, AIS security has its own terminology and jargon. To carry out your AIS responsibilities, you need to be familiar with these terms and their meanings.

AIS SECURITY CONCEPTS

Our AIS security goal is to take all reasonable measures to protect our AIS assets. Keep in mind that AIS assets (hardware, software, data, supplies, documentation, people, and procedures) have value.

Their value can usually be stated in dollar terms. It costs money to repair or replace hardware. It costs money to reprogram and redocument. It costs money to retrain personnel. Unauthorized access costs money. Service delays cost money.

AIS Assets

Our AIS assets (figure 4-1) include the facilities, hardware, software, data, supplies, documentation, people and procedures. These assets combine to provide service. Service is computer time, telecommunications, data storage, user support, application system development, and operation. Service must be available to those authorized to receive it when they request it. Information is at the top of the triangle. It is the ultimate AIS asset. Information is the reason the rest exists.

Threats

Threats are things that can destroy your assets (figure 4-2). Easy to recognize, threats come in two basic forms: people and environmental changes. People are a threat because they sometimes do unexpected things, make mistakes, or misuse resources, steal, subvert, and sabotage (deliberate threats). Some of us even smoke and spill soft drinks in computer rooms. Environmental threats are things like heat, humidity, explosions, dust, dirt, power peaks, power failures; and natural disasters like fire, floods, hurricanes, thunderstorms, and earthquakes. Hardware

failures and compromising emanations are also threats. Another term associated with threats is their probability of occurrence. What is the likelihood that something will happen? Probabilities are measured in time—once a pico second, once a memory cycle, once a fiscal year, once a century.

Vulnerability

Threats cannot reach an AIS asset without the aid and assistance of a vulnerability. Vulnerabilities are the holes threats sneak through or weaknesses they exploit. Vulnerabilities are caused by lack of AIS security planning, poor management, disorganization, disorder, inadequate or improper procedures, open data and open door policies, undocumented software, unaware or unconcerned personnel. You can help limit the vulnerabilities by following established AIS security policies and procedures.

Successful Attacks and Adverse Events

Successful attacks and adverse events result from a combination of threats, vulnerabilities, and AIS assets. When a threat takes advantage of a vulnerability and does harm to your AIS assets, a successful attack or adverse event has occurred. Successful attacks and adverse events may be roughly grouped as losses or abuses. You can lose hardware, software, and data. You can lose documentation and supplies. You can lose key staff personnel. Losses often result in denial of service, preventing access to information when it is

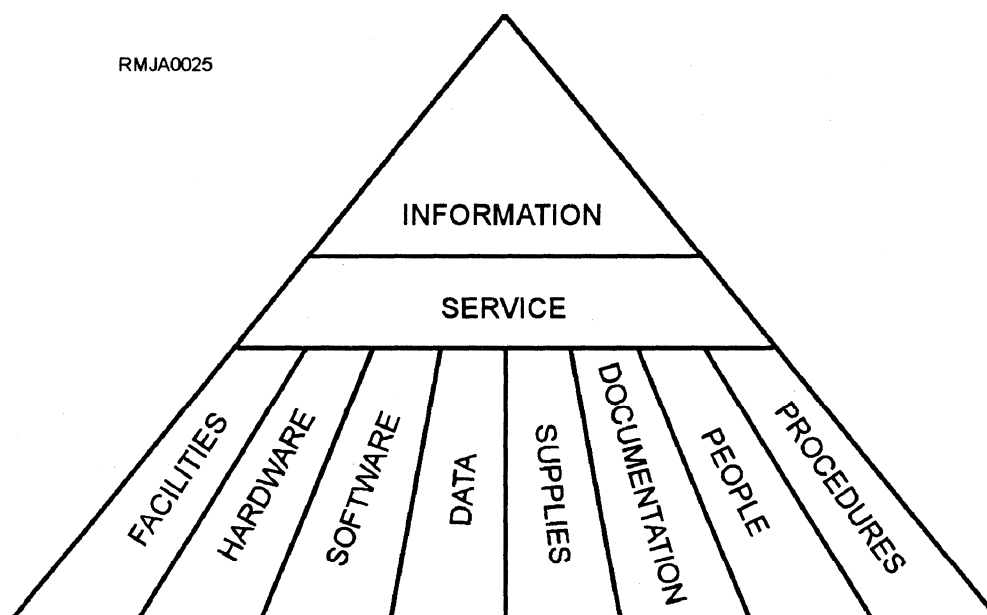


Figure 4-1.—AIS assets.

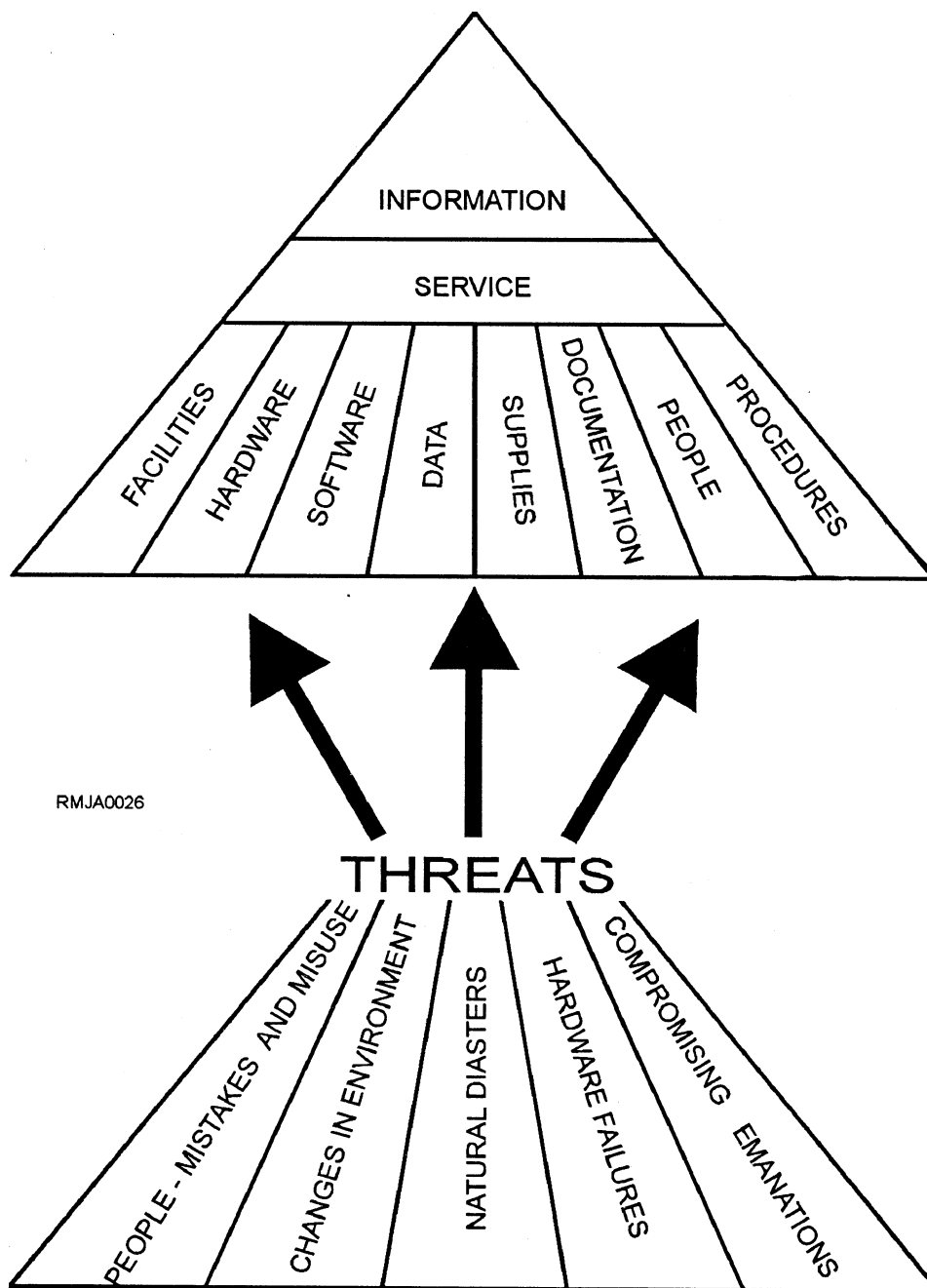


Figure 4-2.—Threats to AIS assets.

needed. Abuse relates to unauthorized access to service, unwanted destruction or alteration of data and software, and unauthorized disclosure of classified information.

We have an adverse event with every fire and with every flood caused by a broken pipe in a computer room. We have a successful attack with every bowling score, recipe, or school paper stored online, and with every computer hacker that plays crash-the-computer or scramble-the-data.

Likelihood and Risk

Likelihood and risk relate to successful attacks and adverse events. Likelihood relates to chance—what is the likelihood (probability) that a successful attack or an adverse event will occur? Risk has to do with money; it tells us about the cost of loss or abuse from an adverse event overtime. We first ask, “What is the value of the AIS asset that will be abused or that we will lose if a given successful attack or adverse event occurs?” Then we ask, “How often can we expect that

particular attack or event to occur?” Remember, the successful attack or adverse event results from a particular threat exploiting a particular vulnerability. It is very specific reasoning. The greater the value of the AIS asset and the more likely the successful attack or adverse event, the greater the risk. Figure 4-3 shows this risk analysis concept. Risks are usually expressed in terms of dollars per year, the annual loss expectancy.

Countermeasures

Once the threats and vulnerabilities are known and the likelihood and risk of a successful attack or an adverse event are determined, a plan is developed to set up countermeasures (controls) to lessen or eliminate the vulnerabilities. If you have a countermeasure, you have a protected vulnerability. If you have an unprotected vulnerability, you do not have a countermeasure. Some countermeasures help us prevent adverse events, whereas others detect adverse events. We have measures to minimize the effects of successful attacks or adverse events. We also have measures, called contingency plans, to recover from a successful attack or an adverse event. Figure 4-4 gives an example of each type of security measure strategy as it relates to fire loss. Figure 4-5 shows threats, vulnerabilities, and countermeasures to our assets.

Another way to categorize countermeasures is by type: physical, technical, administrative, and managerial (figure 4-6).

PHYSICAL CONTROLS.— We usually think of physical control first. They include the locked computer room door, physical layout, fire extinguishers, access barriers, air conditioners, moisture detectors, and alarms.

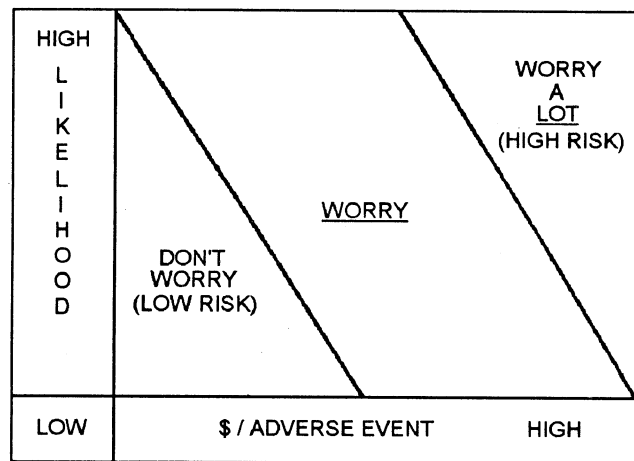


Figure 4-3.—AIS security risk analysis.

TECHNICAL CONTROLS.— Technical controls are embedded in hardware, software, and telecommunications equipment. They are diagnostic circuitry, component redundancies, and memory protect features. They are controls built into the operating system. They include log-on IDs and passwords to enable only authorized users access to the computer system. They are accounting routines, encryption coding, and audit trails.

ADMINISTRATIVE CONTROLS.— Administrative controls concern people and procedures. They include who is authorized to do what, methods to keep track of who enters a sensitive area, who receives a delivery, and who requests a sensitive report. The operating procedures you follow will sometimes include security requirements. You are responsible for adhering to the procedures to ensure AIS requirements are met.

MANAGERIAL CONTROLS.— Managerial controls tie everything together. They concern planning and evaluation. They include audits to review the effectiveness and efficiency of the countermeasures. They check to make sure that the measures are actually in place, being followed, and working. Problems found require replanning and reevaluation to see that corrections are made.

RISK MANAGEMENT

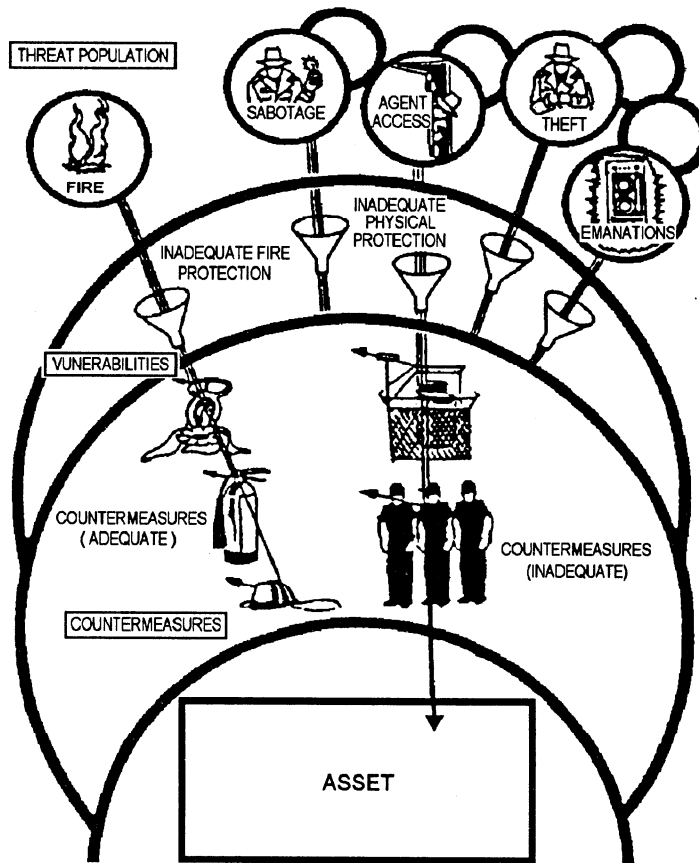
Risk management involves assessing the risks, determining loss potential estimates, and selecting countermeasures appropriate to prevent, detect, minimize, and recover from successful attacks and adverse events. Management selects the countermeasures, making sure that the cost of the measure is less than the cost of the risk. The trick is to select the countermeasure that will result in the lowest total cost while taking all reasonable measures to protect our AIS assets.

Keep in mind that the presence of a vulnerability does not in itself cause harm. A vulnerability is merely a condition or set of conditions that may allow the computer system or AIS activity to be harmed by an attack or event. Also, keep in mind that an attack made does not necessarily mean it will succeed. The degree of success depends on the vulnerability of the system or activity and the effectiveness of existing countermeasures. Countermeasures may be any action, device, procedure, technique, or other measure that reduces the vulnerability of an AIS activity or computer system to the realization of a threat.

COUNTERMEASURE STRATEGY FOR FIRE LOSS			
PREVENT	DETECT	MINIMIZE	RECOVER
CLEAN ROOM	SMOKE DETECTOR	HALON	CONTINGENCY PLAN
SECURE CABLES AND CONNECTIONS		OFF-SITE DATA STORAGE	ALTERNATE COMPUTER USE
NO SMOKING			

RMJA0028

Figure 4-4.—An example of countermeasures against fire loss.

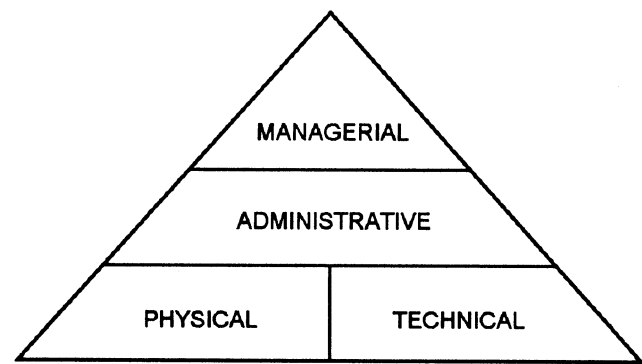


RMJA0029

Figure 4-5.—Threats, vulnerabilities, and countermeasures.

Not all attacks and events can be avoided. If we cannot reasonably prevent something, we want to detect the problem as early as possible, minimize the damage and destruction, and recover as quickly and efficiently as possible. To help us minimize and recover, we develop contingency plans.

Contingency plans (backup plans) provide for the continuation of an activity's mission during abnormal operating conditions. These are plans for emergency response, backup operations, and post-disaster recovery. They include a preparation phase that includes the steps to be taken in anticipation of a loss to



RMJA0030

Figure 4-6.—Types of AIS security countermeasures.

lessen damage or assist recovery. The action phase includes the steps to be taken after a successful attack or adverse event to minimize the cost and disruption to the AIS environment.

SCOPE OF AIS SECURITY

As the Navy has become increasingly dependent on the use of AIS for its payroll, supply functions, tactical information, and communications, the need to protect AIS assets has taken on greater importance. Risk management is an ongoing effort. Whether you are in a large AIS facility with a full-time information system security manager (ISSM) or a facility where the functions of the ISSM are a collateral duty, your installation will have established security measures to protect its AIS assets.

The five areas of consideration for the Navy's AIS security program are hardware (I), data (II), human resources (III), software (IV), and communications (V). These are shown in figure 4-7. Because each AIS facility is different, each facility has its own AIS security risk management program. You'll be responsible for following the requirements of your facility's AIS security program.

In the next paragraphs, you will learn about management responsibilities, your responsibilities, physical security measures, and data security measures. Again, our goal in AIS security is to prevent or minimize the opportunity for modification, destruction, disclosure, or denial of service.

MANAGEMENT RESPONSIBILITY

AIS security is everyone's responsibility, and only the commanding officer (CO) can ensure that AIS security receives the support required at every level. The success of your command's AIS security program depends upon the support of the CO. The CO and the AIS security staff are responsible for taking the necessary steps to provide an adequate level of security for all AIS-related activities, automated information systems, and networks, including those developed, operated, maintained, or provided by contractors.

Each AIS facility has an information system security manager (ISSM). His or her primary duty is to serve as the single point of contact for all matters relating to AIS security at your command. The ISSM usually reports directly to the CO. Now, let's talk a little about the security staff.

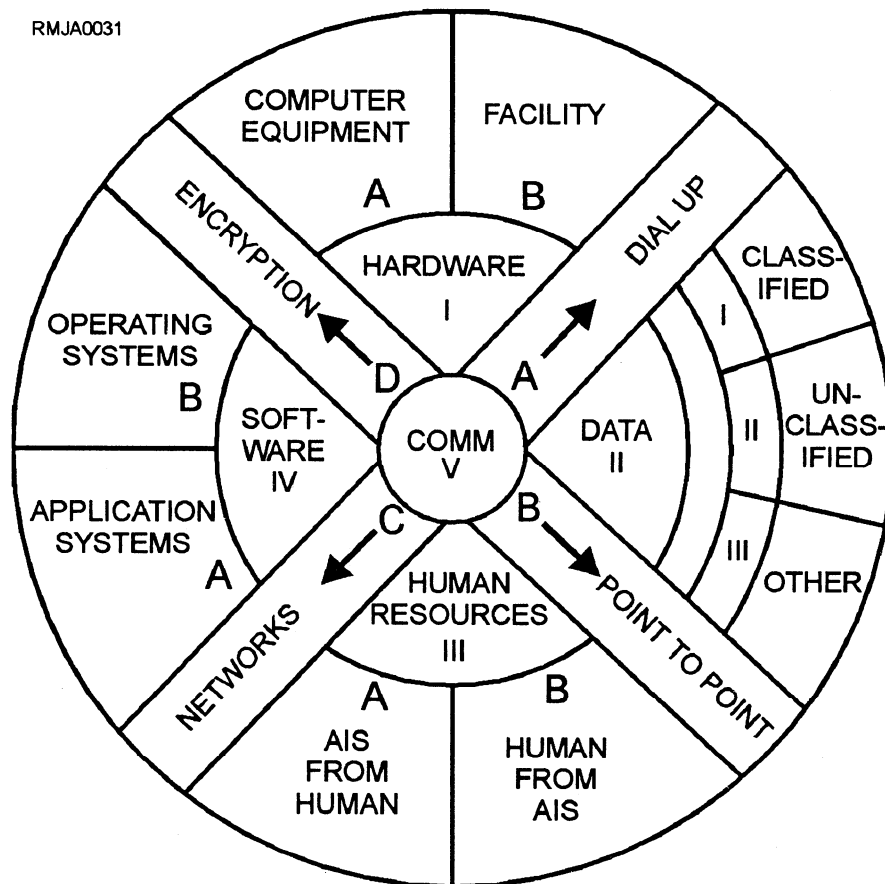


Figure 4-7.—Department of the Navy AIS security areas.

Many factors determine the numbers and types of people assigned to the AIS security staff. These factors include the type of activity, its size, its hardware configuration(s), types of work to be processed, and so on. Your command's AIS security staff may include any one, several, or all of the following people:

- Command security manager;
- Information system security manager (ISSM);
- Information system security officer (ISSO);
- Network security officer (NSO);
- Terminal area security officer (TASO).

These people are specialists. Some day you may be one of them. They have been trained and are knowledgeable in such areas as the following:

- General security awareness;
- User and customer security;
- Security administration;
- Security violation reporting;
- Hardware and software security;
- Systems design security;
- Terminal and device related security;
- Telecommunications security;
- Physical security;
- Personnel security;
- Computer auditing;
- Data security;
- Risk assessment methodology;
- Contingency and backup planning;
- AIS security and Navy contractors;
- Disaster recovery;
- Security accreditation; and
- Security test and evaluation.

From this list you can see that AIS security is a complex area and requires many specialized skills and knowledges. In addition, each member of the AIS security staff is responsible for ensuring that you are adequately trained in AIS security. Do you know the name of your command ISSM? If not, seek him or her

out and find out what your responsibilities are, rather than finding out the hard way through a bad experience. That brings us to your responsibilities.

PERSONAL RESPONSIBILITY

You play an important role in the success of your command's security program. As we stated earlier, security is everybody's job, from seaman recruit to admiral.

Do not leave listings unattended or files open for unauthorized browsing. If you see a stranger in your work area, it is your job to confront (challenge) that individual regardless of his or her rate or rank, job title, or status within or outside of your command. For the most part, you know who is authorized to be in your work area.

As a computer operator, you are responsible for protecting hardware from fire, flood, sabotage, and internal tampering. You are also concerned with protecting applications software, systems software, program and data files, and all forms of input and output media with which you will be working.

If you are working in the magnetic media library, you are responsible for protecting all library-related equipment (tape/disk cleaners, tape degaussers, tape/disk certifiers, and so on). If you are handling and working with classified media and materials, you must handle, store, and dispose of them in accordance with established procedures. The same rules apply regardless of what area you maybe working in; whether you are a data entry operator, a control clerk in production control (I/O), a computer programmer, or an analyst. All positions require you to pay attention to AIS security. The key word is *protect*.

Believe it or not, AIS security is not really that difficult to understand, nor is it difficult to carry out. Sixty-five percent of it is nothing more than using good old common sense; the remaining thirty-five percent comes from awareness that you get through proper training.

Try thinking of AIS security and protecting its related assets the same way you would protect your home and personal effects. In AIS we are talking millions of dollars, some of them yours. Think about the kind of AIS security you would want to have installed if that AIS facility were yours and what you would do to protect all its assets.

From this point on, the rest is up to you. Stay alert, keep your eyes and ears open to what is going on around

you, and never hesitate to challenge or question someone or something that you feel is wrong or out of character.

PHYSICAL SECURITY MEASURES

Physical security is the one area with which you are most likely to be familiar. It deals with such things as personnel, the environment, the facility and its power supply(ies), fire protection, physical access, and even the protection of software, hardware, and data files.

Your command must provide physical security for your AIS facility. The degree of physical security at your installation or command depends on its physical characteristics, its vulnerability within the AIS environment, and the type of data processed. Minimum physical security requirements include four basic areas that your command must address: physical security protection, physical access controls, data file protection, and natural disaster protection.

- **Physical security protection.** Physical security protection takes on two forms. The first is physical barriers, such as solid walls, caged-in areas, bulletproof glass, locked doors, and even continual surveillance of the controlled area. The second involves people and the procedures that you must follow, such as looking up names on the access list to determine who is authorized in a given space or area. There are also escort procedures you must follow to be sure that your party gets to the right place and/or person.
- **Physical access controls.** Physical access controls are implemented to prevent unauthorized entry to your computer facility or remote terminal areas. Physical access controls can be accomplished in several ways: conventional key and lock set, electronic key system, mechanical combination lock, or electronic combination lock. Regardless of the type of system installed at your command, it is important to remember that keys belong on your key-ring or chain, electronic keys or cards should be in your possession at all times (except when sleeping), and combinations should be memorized, not written down somewhere for everyone to see.
- **Data file protection.** Physical access to data files and media libraries (magnetic disks, tape files, microforms, and so on) is authorized only to those personnel requiring access to perform their job.

- **Natural disaster protection.** The effects of natural disasters must be prevented, controlled, and minimized to the extent economically feasible by the use of detection equipment (heat sensors, smoke detectors), extinguishing systems, and well conceived and tested contingency plans.

Environmental Security

Temperature and humidity can affect the operation of your computer facility. Whenever possible, computer equipment is operated within the manufacturer's optimum temperature and humidity range specification. Fluctuations in temperature and/or humidity over an extended period of time can cause serious damage to the equipment. So, with that in mind, you are probably asking yourself, "What are the acceptable levels for computer operation?" Normally, you can find this information in the command's standard operating procedures (SOPs), or you can check with your supervisor. If neither are available, a safe rule of thumb is a temperature of 72° Fahrenheit, $\pm 2^\circ$, and a humidity of 55%, $\pm 5\%$.

To maintain a constant temperature and humidity to the computer facility or remote terminal areas, keep all doors and windows closed. Because temperature and humidity are vitally important to computer performance, it is essential that only designated personnel be allowed to regulate these types of environmental controls.

If your workspace has a recording instrument to monitor the temperature and humidity, by all means check it periodically to be sure it is within the prescribed limits. If you notice a significant fluctuation (up or down), notify your supervisor.

Some devices have built-in warning signals (a light, audible sound, or both) to warn you of near-limit conditions for temperature and/or humidity.

Lighting

You are responsible for ensuring that adequate lighting is maintained. Be particularly attentive to emergency lights. If they are not functioning properly, report the problem to your supervisor as soon as possible. Emergency lights are installed for your protection and safety, not for the safety of the equipment. They are there to ensure a quick exit if you must evacuate in a hurry.

Physical Structure Security

In the Navy we often decide we need computer equipment and then wonder where we are going to install it. The existing building (or shipboard compartment) may not lend itself to the physical security requirements needed to protect the system.

Things like false overheads (ceilings) can conceal water and steam pipes. The pipes should be checked on a regular basis and any irregularities reported immediately. Personnel should be familiar with the locations and operation of the cut-off valves for the pipes. Air-conditioning ducts in the overhead, if not properly insulated, can result in condensation, causing water to drip down on the computer.

When repair work is scheduled within the computer spaces (working under the raised floor or in the overhead), be sure to take all necessary precautions to protect the equipment. Use plastic sheeting to cover the system (particularly the CPU). Watch out for overhead water or steam pipe bursts and for activated sprinkler systems. Ensure maximum personnel safety, while keeping disruption to a minimum. Dust coming from the work area can damage the equipment: clogged filters result in overheated components, a head crash on a disk drive, dirty read/write heads on tape drives, and so on. Remember, the key word is to protect all AIS assets.

WARNING

Should your equipment be exposed to water, do not turn it on until it has been thoroughly checked out by qualified maintenance personnel.

Power Supply Protection

Your computer facility and remote terminal areas require adequate power. Variations in electrical power can affect the operation of computer equipment. Most computer equipment is designed in such away that it is able to rectify the incoming ac current, filter it, and regulate the resulting dc current before it is applied to the computer circuitry. However, this filtering and regulation cannot be expected to eliminate voltage variations beyond a reasonable range. Power fluctuations can cause unpredictable results on hardware, logic, and data transfer. Should your system encounter such fluctuations, it is highly recommended that the equipment be shut down at once until the problem is corrected.

Some computer systems are equipped with an uninterrupted power source (UPS). A UPS provides the auxiliary power for your equipment that may be required if your command's mission dictates continuous AIS support to fulfill its obligations or if your computer system is in an area where there are frequent brownouts. Auxiliary power should be checked on a periodic basis.

Fire Protection

Fire protection is one of the major elements of any command's physical security program. All personnel (military and civilian) receive periodic training in emergency procedures in case of fire. The training usually includes, at a minimum, proper equipment shutdown and startup procedures, information about your fire detection and alarm systems, use of emergency power (especially aboard ship), use of fire-fighting equipment, and evacuation procedures.

Master control switches are used to shut off all power to your AIS spaces in the event of fire. If your air-conditioning system is not setup for smoke removal, it is probably connected to the master control switches. The master control switches are normally located at the exit doors, so in an actual emergency you do not have to pass through a dangerous area to activate the switches. These switches should be easily recognizable. They are clearly labeled and protected to prevent accidental shutdown. Commands that process critical applications will have master control switches that allow for a sequential shutdown procedure of your equipment. Learn the location of the switches and procedures used in your computer spaces.

There will be enough portable fire extinguishers for you to fight a relatively small or self-contained fire. Extinguishers are placed within 50 feet of the computer equipment. Prominently displayed markings and/or signs are above each extinguisher, and each is easily accessible for use.

WARNING

Be sure to use only carbon dioxide or inert-gas fire extinguishers on electrical fires.

One final note. Experience has shown repeatedly that prompt detection is a major factor in limiting the amount of fire damage. Computer areas require a fire detection system capable of early warning and with an automatic fire extinguishing system.

Hardware Protection

Hardware security is defined in the *Department of the Navy Automatic Data Processing Security Program*, OPNAVINST 5239.1, as “Computer equipment features or devices used in an AIS system to preclude unauthorized, accidental or intentional modification, disclosure, or destruction of AIS resources.”

DATA PROTECTION MEASURES

FIPS (Federal Information Processing Standards) PUB 39 *Glossary for Computer Systems Security* defines data security as “The protection of data from unauthorized (accidental or intentional) modification, destruction, or disclosure.” We are always concerned with the integrity of data; is the data the same as that in the source documents? We want to ensure that the data has not been exposed to accidental or intentional modification, disclosure, or destruction.

Depending on the type of data being processed, the other users with access to the system, and the technical features of the system to provide the needed safeguards, the system may have to operate in a specific security mode.

If your command processes classified and/or sensitive unclassified data, it must abide by certain rules to protect it. In the central computer facility (where the host computer is located), the physical security requirements will be equal to the highest classification of data being handled. If there are two or more computer systems located in the same controlled area, the systems should be separated to limit direct personnel access to a specific system.

In remote terminal areas, security requirements are based upon the highest classification of data to be accessed through the terminals. Each remote terminal must be identifiable through hardware or software features when it is connected to a computer system or network processing classified data. The system or network must know who is logging on.

If the computer system to which your remote terminal is connected is processing classified data and your terminal is not authorized, controlled, or protected for that classification of data, it must be disconnected. The disconnect procedures may be by a hardware measure (such as turning off a switch at the host computer) or a software measure (such as deleting the ID of your terminal during certain processing periods). Because each data classification has different security requirements, we cover each separately.

Classified Data

Handling requirements and procedures for classified AIS media (Confidential, Secret, and Top Secret) are the same as those for handling classified information. Anyone who has possession of classified material is responsible for safeguarding it at all times. You need to be familiar with the four security modes that provide for processing classified data: system high, dedicated, multilevel, and controlled.

SYSTEM HIGH SECURITY MODE.— A computer system is in the system high security mode when the central computer facility and all of the connected peripheral devices and remote terminals are protected in accordance with the requirements for the highest classification category and type of material then contained in the system. All personnel having computer system access must have a security clearance, but not necessarily a need-to-know for all material then contained in the system. In this mode, the design and operation of the computer system must provide for the control of concurrently available classified material in the system on the basis of need-to-know.

DEDICATED SECURITY MODE.— A computer system is operating in the dedicated security mode when the central computer facility and all of its connected peripheral devices and remote terminals are exclusively used and controlled by specific users or group of users having a security clearance and need-to-know for the processing of a particular category(ies) and type(s) of classified material.

MULTILEVEL SECURITY MODE.— A computer system is operating in the multilevel security mode when it provides a capability permitting various categories and types of classified materials to be stored and processed concurrently in a computer system and permitting selective access to such material concurrently by unclassified users and users having differing security clearances and need-to-know. Separation of personnel and material on the basis of security clearance and need-to-know is accordingly accomplished by the operating system and associated system software. In a remotely accessed resource-sharing system, the material can be selectively accessed and manipulated from variously controlled terminals by personnel having different security clearances and need-to-know. This mode of operation can accommodate the concurrent processing and storage of (1) two or more categories of classified data, or (2) one or more categories of classified data with unclassified data, depending upon the constraints

placed on the system by the designated approving authority.

CONTROLLED SECURITY MODE.— A computer system is operating in the controlled security mode when at least some personnel (users) with access to the system have neither a security clearance nor a need-to-know for all classified material then contained in the computer system. However, the separation and control of users and classified material on the basis, respectively, of security clearance and security classification are not essentially under operating system control as in the multilevel security mode.

Sensitive Unclassified Data

Sensitive unclassified data is unclassified data that requires special protection. Examples are data For Official Use Only and data covered by the Privacy Act of 1974.

The Privacy Act of 1974 imposes numerous requirements upon federal agencies to prevent the misuse of data about individuals, respect its confidentiality, and preserve its integrity. We can meet these requirements by applying selected managerial, administrative, and technical procedures which, in combination, achieve the objectives of the Act.

The major provisions of the Privacy Act that most directly involve computer security are as follows:

- Limiting disclosure of personal information to authorized persons and agencies;
- Requiring accuracy, relevance, timeliness, and completeness of records; and
- Requiring the use of safeguards to ensure the confidentiality and security of records.

To assure protection for AIS processing of sensitive unclassified data, the Navy has established the limited AIS access security mode.

A computer system or network is operating in the limited access security mode when the type of data being processed is categorized as unclassified and requires the implementation of special access controls to restrict the access to the data only to individuals who by their job function have a need to access the data.

Unclassified Data

Although unclassified data does not require the safeguards of classified and sensitive unclassified data, it does have value. Therefore, it requires proper

handling to assure that it is not intentionally or unintentionally lost or destroyed.

AIS MEDIA PROTECTION MEASURES

AIS media protection is important because that is where we store data, information, and programs. All data and information, whether classified or not, require some degree of protection. Software also requires protection. You would not want to lose the only copy of a program you had worked 4 months to write, test, and debug. The amount of protection depends on the classification of data, the type of AIS storage media used, the value of the material on it, and the ease with which the material can be replaced or regenerated. AIS media includes magnetic tapes, disks, diskettes, disk packs, drums, cathode-ray tube (CRT) displays, hard copy (paper), core storage, mass memory storage, printer ribbons, carbon paper, and computer output microfilm and microfiche.

You are responsible for controlling and safeguarding (protecting) the AIS media at all times. For purposes of control, AIS media can be divided into two types or categories: working copy media and finished media. You will be working with both.

Working copy media is temporary in nature. It is retained for 180 days or less and stays within the confines and control of your activity. Examples of working copy media are tapes and disk packs that are used and updated at frequent intervals and coding forms that are returned immediately to the user after processing.

Finished media is permanent in nature. It includes tapes and disk packs, hard-copy output, or any other AIS media containing data or information to be retained for more than 180 days. Finished media can be released to another activity. For example, a magnetic tape can be sent to another activity as a finished media. However, the receiving activity may treat it as working copy media if it is kept 180 days or less. Of course, AIS media, whether working copy or finished copy, requires the use of security controls.

Security Controls

The security controls we discuss are general in nature and are considered the minimum essential controls for protecting AIS media. Your activity's standard operating procedures (SOPS) are designed to ensure that an adequate level of protection is provided. Classified working copy media must be dated when created, marked, and protected in accordance with the

highest classification of any data ever recorded on the media. If classified working copy media is given to a user, the user is then responsible for its protection.

Classified finished media must be marked and accounted for. You may be responsible for inventorying magnetic tapes, disk packs, and other forms of AIS media. Your activity must maintain a master list of AIS media that is classified as Secret or Top Secret. This master list includes the overall security classification of the media and the identification number permanently assigned to it. The media must also be controlled in the same manner prescribed for classified material outside an AIS environment. For additional information, consult the *Department of the Navy Information and Personnel Security Program Regulation*, OPNAVINST 5510.1 (hereinafter called the *Security Manual*).

Security Markings

Your activity will have procedures for marking AIS media. These are important to protect the media from unauthorized, accidental, or intentional disclosure, modification, destruction, or loss. You can imagine how easy it is to pickup an unmarked tape, load it on the tape drive, and have whatever is on it recorded over by a program. You have probably done this to tapes with your tape cassette recorder/player. This is why we have mechanical means, like tape rings and diskette notches, to protect magnetic media. These methods, combined with clearly marked labels, go a long way toward protecting data and programs on magnetic media. Let's look at the types of markings the Navy uses for the various types of media for marking classified data.

MAGNETIC MEDIA.— Each magnetic tape, diskette, and disk pack must be externally marked with a stick-on label with the overall security classification and a permanently assigned identification number. When the tapes, diskettes, and disk packs are to be declassified by degaussing, all external labels indicating the classification must be removed unless the media will be immediately used to store information of the same classification. Many installations set aside groups of tapes and disks for recording classified data at each security level.

HARD-COPY REPORTS, MICROFILM, AND MICROFICHE.— Hard-copy reports or printouts from a printer, terminal, plotter, or other computer equipment and microfilm and microfiche must be properly marked. Those prepared during classified processing must be marked at the top and bottom of

each page with the appropriate classification or the word “unclassified,” and each page should be consecutively numbered.

CRT DISPLAYS.— The appropriate security classification marking is displayed at the top of the screen when displaying classified data or information.

Disposition of Media

There comes a time when the media or the information on the media is no longer needed. With microfilm, microfiche, and printouts, we destroy the media with the data. The same is not true of magnetic media. We can erase and reuse the media when the data is no longer needed. However, the media cannot function forever. Tapes and disks become damaged or eventually wear out.

When a disk or tape becomes unusable, it must be disposed of. But first, each disk and tape must be accounted for. It may have been used for classified data. The magnetic media librarian will see that it is disposed of properly. If the media contained classified data, it will be degaussed before being destroyed.

There are two other problem areas we tend to forget: printer ribbons and carbon paper. Ribbons and carbon paper must be disposed of properly. Because of the large variety of ribbons and printers, it is difficult to state with certainty that any and all classified information have been totally obscured from a given ribbon unless you examine that ribbon in detail. Therefore, printer ribbons are controlled at the highest classification of information ever printed by that ribbon until that ribbon is destroyed. The same ribbon is used in the printer for classified and unclassified information consistent with the levels of physical security enforced for the area.

Carbons are easily readable and must be handled and disposed of in accordance with the classification of data they contain. Remember, regardless of what the media is, it must be disposed of in accordance with the *Security Manual* if it ever contained classified information.

Basically, the requirement states that the data must be destroyed beyond recognition. If the media did not contain classified information, follow your activity's standard operating procedures (SOPs).

AIS SECURITY PROGRAM IMPLEMENTATION

The risk analysis and higher authority instructions provide the basis for an AIS security program. Even though implementation of the program depends on local instructions/directives and conditions, it may not be clear just where to begin.

AIS SECURITY PROGRAM PLANNING

Following is a suggested outline to use as a basis for planning an AIS security program:

- **Perform preliminary planning.** Establish an AIS security team to prepare an AIS security program and make responsibility assignments.
- **Perform a preliminary risk analysis.** This will identify major problem areas.
- **Select and implement urgent “quick fix” security measures.** This should be done on an as-needed basis.
- **Perform and document a detailed risk analysis.** This will allow for review and approval.
- **Justify cost and document action plans.** Based on the approved risk analysis selected, develop budgets and schedules for security measures, contingency plans, training and indoctrination plans, and test plans.
- **Carry out the approved action plans.**
- **Repeat the detailed risk analysis and subsequent steps regularly, at least annually.** Conduct more frequently if required based on the results of tests, inspections, and changes in mission or environment.

AIS SECURITY PLAN DOCUMENTATION

Include adequate documentation in the action plans. For example, the documentation might include the following:

- A security policy statement that provides general guidance and assigns responsibilities;
- A security handbook (with instructions) that describes in detail the security program and procedures and the obligations of AIS personnel, users, and supporting personnel;

- Command standards for system design, programming, testing, and maintenance to reflect security objectives and requirements;
- Contingency plans for backup operations, disaster recovery, and emergency response; and
- Booklets or command instructions for AIS staff indoctrination in security program requirements.

Depending on the normal practices of the AIS facility, these documents may be completely separate items or they may be included in other documents. For example, emergency response plans for the AIS facility might be included in the command’s Disaster Control Plan. Similarly, security standards could be added to existing documents.

The final point to be made is the importance of continuing the inspection and review of the security program. A major effort is required for the initial risk analysis, but once it is completed, regular review and updating can be done much more quickly. By evaluating changes in command mission, the local environment, the hardware configuration, and tasks performed, the AIS technical manager can determine what changes, if any, should be made in the security program to keep it effective.

AUTHORITATIVE REFERENCES

Numerous higher authority instructions relate to physical security, data protection, and security in general. You should have a thorough knowledge of them before implementing any security plan. Refer to the following instructions and manuals to learn about AIS security and when making security decisions:

- *Department of the Navy Automatic Data Processing Security Program*, OPNAVINST 5239.1 with enclosures;
- *Guideline for Automatic Data Processing Risk Analysis*, FIPS PUB 65 (enclosure 3 to OPNAVINST 5239.1);
- *Department of the Navy Information and Personnel Security Program Regulation*, OPNAVINST 5510.1;
- *Department of the Navy Information Systems Security (INFOSEC) Program*, SECNAVINST 5239.3.

AIS THREATS AND RISK ANALYSIS

First, when designing its security program, a command must look at the potential AIS threats and perform a risk analysis.

AIS THREATS

When planning a security program, the AIS technical manager should be aware of all the types of threats that may be encountered. Not every Navy AIS facility will be faced with each type of threat, especially if the facility is aboard ship. The impact of a given threat may depend on the geographical location of the AIS facility (earthquakes), the local environment (flooding), and potential value of property or data to a thief, or the perceived importance of the facility to activists and demonstrators or subversives. Examples of natural and unnatural threats include:

- Unauthorized access by persons to specific areas and equipment for such purposes as theft, arson, vandalism, tampering, circumventing of internal controls, or improper physical access to information;
- AIS hardware failures;
- Failure of supporting utilities, including electric power, air conditioning, communications circuits, elevators, and mail conveyors;
- Natural disasters, including floods, windstorms, fires, and earthquakes;
- Accidents causing the nonavailability of key personnel;
- Neighboring hazards, such as close proximity to chemical or explosive operations, airports, and high crime areas;
- Tampering with input, programs, and data; and
- The compromise of data through interception of acoustical or electromagnetic emanations from AIS hardware.

The preceding list of threats to the operation of an AIS facility contains only a few of the reasons why each command should have an ongoing security program adapted and tailored to its individual needs and requirements. Not all threats and preventive measures can be discussed in this chapter. However, we will cover the more common threats and remedial measures. For a thorough review of the subject, refer to the

Department of the Navy Physical Security and Loss Prevention, OPNAVINST 5530.14.

RISK ANALYSIS

The AIS facility upper management should begin development of the security program with a risk analysis. A risk analysis, as related to this chapter, is the study of potential hazards that could threaten the performance, integrity, and normal operations of an AIS facility. Experience at various commands shows that a quantitative risk analysis produces the following benefits:

- Objectives of the security program relate directly to the missions of the command.
- Those charged with selecting specific security measures have quantitative guidance on the type and amount of resources the AIS facility considers reasonable to expend on each security measure.
- Long-range planners receive guidance in applying security considerations to such things as site selection, building design, hardware configurations and procurements, software systems, and internal controls.
- Criteria are generated for designing and evaluating contingency plans for backup operations, recovery from disaster, and dealing with emergencies.
- An explicit security policy can be generated that identifies what is to be protected, which threats are significant, and who will be responsible for executing, reviewing, and reporting the security program.

Loss Potential Estimates

The first step to consider when preparing the risk analysis is to estimate the potential losses to which the AIS facility is exposed. The objective of the loss potential estimate is to identify critical aspects of the AIS facility operation and to place a monetary value on the loss estimate. Losses may result from a number of possible situations, such as:

- **Physical destruction or theft of tangible assets.** The loss potential is the cost to replace lost assets and the cost of delayed processing.
- **Loss of data or program files.** The loss potential is the cost to reconstruct the files, either

from backup copies if available or from source documents and possibly the cost of delayed processing.

- **Theft of information.** The loss potential because of theft is difficult to quantify. Although the command itself would sustain no direct loss, it clearly would have failed in its mission. In some cases, information itself may have market value. For example, a proprietary software package or a name list can be sold.
- **Indirect theft of assets.** If the AIS is used to control other assets, such as cash, items in inventory, or authorization for performance of services, then it may also be used to steal such assets. The loss potential would be the value of such assets that might be stolen before the magnitude of the loss is large enough to assure detection.
- **Delayed processing.** Every application has some time constraint, and failure to complete it on time causes a loss. In some cases the loss potential may not be as obvious as, for example, a delay in issuing military paychecks.

To calculate the loss potential for physical destruction or theft of tangible assets, AIS technical managers and upper management should construct a table of replacement costs for the physical assets of the AIS facility. The physical assets usually include the building itself and all its contents. This tabulation, broken down by specific areas, helps to identify areas needing special attention. While the contents of the typical office area may be valued at \$100 to \$500 per square foot, it is not unusual to find the contents of a computer room are worth \$5,000 to \$10,000 per square foot. The estimate is also helpful in planning for recovery in the event of a disaster.

The remaining four loss potential types listed are dependent on the characteristics of the individual data processing tasks performed by the AIS facility. AIS technical managers should review each task to establish which losses a facility is exposed to and which factors affect the size of the potential loss. Call on users to help make these estimates.

To make the best use of time, do a rapid, preliminary screening to identify the tasks that appear to have significant loss potential. An example of preliminary estimates is shown in table 4-1.

Having made a preliminary screening to identify the critical tasks, seek to quantify loss potential more precisely with the help of user representatives familiar with the critical tasks and their impact on other activities. Mishaps and losses that could occur should be considered, on the assumption that if something can go wrong, it will. The fact that a given task has never been tampered with, used for an embezzlement, or changed to mislead management in the command is no assurance that it never will be. At this stage of the risk analysis, all levels of management should assume the worst.

Threat Analysis

The second step of the risk analysis is to evaluate the threats to the AIS facility. Threats and the factors that influence their relative importance were listed earlier in this chapter. Details of the more common threats are discussed later in this chapter and, to the extent it is available, general information about the probability of occurrence is given. Use these data and higher authority instructions/manuals and apply common sense to develop estimates of the probability of occurrence for each type of threat.

Table 4-1.—Example of Preliminary Estimates of Loss Potential

TASK NAME	RUN TIME	FILE RECONSTRUCTION	CLASSIFIED/ SENSITIVE DATA	PRIOR COMPROMISE/ THEFT OF INFORMATION	DELAYED PROCESSING IMPACT	PROJECT	MANPOWER COST ESTIMATE
R	1.5/D	Easy	No	No	Extreme	Payroll	1 day
S	Online	Very Difficult	Yes	Yes	Extreme	Operations	1 day
T	2.0/D	Difficult	Yes	No	Moderate	Inventory	7 days
U	0.5/W	Normal	No	No	Low	Research	6 days
V	0.7/M	Difficult	Yes	No	Very low	Research	2 days
W	4.5/W	Easy	No	No	Moderate	Inventory	0.4 day

While the overall risk analysis should be conducted by the AIS technical manager, other personnel at the AIS facility can contribute to the threat analysis, and their help should be requested. Table 4-2 includes a list of common threats at a shore AIS facility, with space for listing the agency or individual to contact should the need arise. Your AIS facility should have a similar list with local contacts of help and information.

Annual Loss Expectancy

The third step in the risk analysis is to combine the estimates of the value of potential loss and probability of loss to develop an estimate of annual loss expectancy. The purpose is to pinpoint the significant threats as a guide to the selection of security measures and to develop a yardstick for determining the amount of money that is reasonable to spend on each of them. In other words, the cost of a given security measure should relate to the loss(es) against which it provides protection.

To develop the annual loss expectancy, construct a matrix of threats and potential losses. At each intersection, ask if the given threat could cause the given loss. For example, fire, flood, and sabotage do not

cause theft-of-information losses; but, in varying degrees, all three result in physical destruction losses and losses because of delayed processing. Likewise, internal tampering could cause an indirect loss of assets. In each case where there can be significant loss, the loss potential is multiplied by the probability of occurrence of the threat to generate an annual estimate of loss.

Remedial Measures Selection

When the estimate of annual loss is complete, AIS upper management will have a clear picture of the significant threats and critical AIS tasks. The response to significant threats can take one or more of the following forms:

- **Alter the environment to reduce the probability of occurrence.** In an extreme case, this could lead to relocation of the AIS facility to a less-exposed location. Alternatively, a hazardous occupancy adjacent to or inside the AIS facility could be moved elsewhere.
- **Erect barriers to ward off the threat.** These might take the form of changes to strengthen the building against the effects of natural disasters,

Table 4-2.—Threat Help List

COMMON THREATS	SOURCES OF LOCAL INFORMATION AND HELP	LOCAL PHONE NUMBER
Fire		
Flood		
Earthquake		
Windstorm		
Power failure		
Air-conditioning failure		
Communications failure		
AIS hardware failure		
Intruders, vandals		
Compromising emanations		
Internal theft		
Internal misuse		

saboteurs, or vandals. (See the *Security Manual* and OPNAVINST 5530.14 for evaluation guidelines.) Special equipment can be installed to improve the quality and reliability of electric power. Special door locks, military guards, and intrusion detectors can be used to control access to critical areas.

- **Improve procedures to close gaps in controls.** These might include better controls over operations or more rigorous standards for programming and software testing.
- **Early detection of harmful situations permits more rapid response to minimize damage.** Fire and intrusion detectors are both typical examples.
- **Contingency plans permit satisfactory accomplishment of command missions following a damaging event.** Contingency plans include immediate response to emergencies to protect life and property and to limit damage, maintenance of plans and materials needed for backup operation offsite, and maintenance of plans for prompt recovery following major damage to or destruction of the AIS facility. The command's Disaster Control Plan should coincide with the AIS facility's contingency plans.

Table 4-3 shows examples of remedial measures for a few threats. When selecting specific remedial measures, use the following two criteria:

1. The annual cost is to be less than the reduction in expected annual loss that could be caused by threats.
2. The mix of remedial measures selected is to be the one having the lowest total cost.

The first criterion simply says there must be a cost justification for the security program—that it returns more in savings to the AIS facility than it costs. This may seem obvious but it is not uncommon for an AIS manager to call for a security measure, to comply with higher authority security instructions and directives, without first analyzing the risks.

The second criterion reflects the fact that a given remedial measure may often be effective against more than one threat. See table 4-3.

Since a given remedial measure may affect more than one threat, the lowest cost mix of measures probably will not be immediately obvious. One possible way to make the selection is to begin with the threat having the largest annual loss potential. Consider possible remedial measures and list those for which the annual cost is less than the expected reduction in annual loss. Precision in estimating cost and loss reduction is not necessary at this point. If two or more remedial measures would cause a loss reduction in the same area, list them all, but note the redundancy. Repeat the process for the next most serious threat and continue until reaching the point where no cost justifiable measure for a threat can be found. If the cost of a remedial measure is increased when it is extended to cover an additional threat, the incremental cost should

Table 4-3.—Example of Remedial Measures by Threat Type

REMEDIAL MEASURES	THREATS				
	Fire	Internal Theft	External Theft	Hurricane	Sabotage
Fire detection system	X				X
Loss control team	X			X	X
Roving guard patrol	X	X	X		X
Intrusion detectors		X	X		X
Personnel screening		X			X
On-site power generator				X	X
Backup plan	X			X	X

be noted. At this point, there exists a matrix of individual threats and remedial measures with estimates of loss reductions and costs, and thus an estimate of the net saving. This is shown graphically in table 4-4.

For each threat (A, B, C, and D), the estimated loss reduction (column 1), the cost of the remedial measure (column 2), and the net loss reduction (column 3) are given in thousands of dollars. By applying remedial measure J to threat A at a cost of \$9,000, a loss reduction of \$20,000 can be expected (a net saving of \$11,000). Furthermore, remedial measure J will reduce the threat B loss by \$10,000 at no additional cost and the threat C loss by \$4,000 at an added cost of only \$1,000. Finally, though, it appears that it would cost more than it would save to apply J to threat D. Therefore, J would not be implemented for D. The net loss reduction from J could be expressed as:

$$\begin{aligned} J(A, B, \& C) &= 11 + 10 + 8 \\ &= \$24,000 \text{ net loss reduction} \end{aligned}$$

The table indicates that J and K have the same reduction effect on threat A. Since K costs more than J, it might, at first glance, be rejected. However,

$$\begin{aligned} K(A, B, C, \& D) &= 5 + 12 + 6 + 2 \\ &= \$25,000 \text{ net loss reduction} \end{aligned}$$

and

$$\begin{aligned} J(A, B, \& C) + K(A, B, C, \& D) &= -4 + 22 + 9 + 2 \\ &= \$29,000 \text{ net loss reduction} \end{aligned}$$

Therefore, while J and K are equally effective on threat A, K appears to be more effective than J on the other threats. Further checking shows their combined use results in the greatest overall net loss reduction.

By going through the process just described, using preliminary estimates for cost and loss reduction, you can test various combinations of remedial measures,

and thus identify the subset of remedial measures that appears to be the most effective. At this point, review the estimates and refine them as necessary to ensure compliance with higher authority security instructions.

If all the preceding procedures are followed, the following factors will be established and documented:

- The significant threats and their probabilities of occurrence;
- The critical tasks and the loss of potential related to each threat on an annual basis;
- A list of remedial measures that will yield the greatest net reduction in losses, together with their annual cost.

With this information at hand, AIS upper management can move ahead with implementing the AIS security program. Since the analysis of remedial measures will have identified those with the greatest impact, relative priorities for implementation can also be established.

AIS DISASTER PROTECTION

Fires, floods, windstorms, and earthquakes all tend to have the same basic effects on AIS operations. They cause the physical destruction of the facility and its contents and interrupt normal operations. They also represent a threat to the life and safety of the AIS staff. To illustrate the effects of the physical destruction of a facility, we have selected fire safety. Other causes of disasters include the loss of support utilities and breaches of AIS facility physical security.

FIRE SAFETY

Experience over the last two decades demonstrates the sensitivity of AIS facilities to fire damage resulting in disruption of operations. A number of major losses

Table 4-4.—Threat Matrix Table

REMEDIAL MEASURES	THREATS											
	A			B			C			D		
	(1)	(2)	(3)	(1)	(2)	(3)	(1)	(2)	(3)	(1)	(2)	(3)
J	20*	9	11	10	0	10	4	1	8	2	5	-3
K	20*	15	5	12	0	12	6	0	6	4	2	2

* Same effect.

have involved noncombustible buildings. In the cases where vital magnetic media tapes were safeguarded and the computer hardware was relatively uncomplicated, rapid recovery was possible, often in a matter of days. However, if a large computer configuration were destroyed or if backup records were inadequate, recovery could take many weeks or months.

Fire safety should be a key part of the AIS facility's security program. It should include the following elements:

- Location, design, construction, and maintenance of the AIS facility to minimize the exposure to fire damage;
- Measures to ensure prompt detection of and response to a fire emergency;
- Provision for quick human intervention and adequate means to extinguish fires; and
- Provision of adequate means and personnel to limit damage and effect prompt recovery.

Facility Fire Exposure

The first factor to consider in evaluating the fire safety of an AIS facility is what fire exposure results from the nature of the occupancy (material) of adjacent buildings and the AIS facility building. Generally speaking, the degree of hazard associated with a given occupancy (material) depends on the amount of combustible materials, the ease with which they can be ignited, and the likelihood of a source of ignition.

The second and third fire safety factors are the design and construction of the building. Five basic types of construction are described in table 4-5, with their approximate destruction times.

Table 4-5.—Estimated Destruction Time by Fire for Selected Construction Types

TYPE OF CONSTRUCTION	APPROXIMATE DESTRUCTION TIME
Fire Resistant	2 or 3 hours
Heavy Timber	1 plus hours
Noncombustible	1 hour
*Ordinary Construction	Less than 1 hour
Wood Frame	Minutes

*Depends on size of timber used

The actual performance of a building will depend not only on the type of construction, but also on design details, such as:

- Fire walls, which, in effect, divide a structure into separate buildings with respect to fires;
- Fire-rated partitions, which retard the spread of a fire within a building;
- Fire-rated stairwells, dampers, or shutters in ducts; fire stops at the junction of floors, and walls and similar measures to retard the spread of smoke and fire within a building; and
- Use of low-flame spread materials for floor, wall, and ceiling finish to retard propagation of flame.

Understand that this discussion is very simplified. However, consideration of these factors as they apply to an existing or projected AIS facility will help to determine the amount of attention to pay to fire safety. Seek the assistance of a qualified fire protection engineer or local base fire personnel in evaluating the inherent fire safety of the AIS facility and identifying hazards.

The fourth factor in fire safety is the way in which the building is operated. Keep in mind that the inherent fire safety of a building can be rendered ineffective by careless operation; for example:

- Fire doors propped open;
- Undue accumulation of debris or trash;
- Careless use of flammable fluids, welding equipment, and cutting torches;
- Substandard electric wiring;
- Inadequate maintenance of safety controls on ovens and boilers; or
- Excessive concentration of flammable materials (AIS facilities, for example, have a particular hazard from the accumulation of lint from paper operations).

The AIS security program should strive, in coordination with the building maintenance staff, to identify and eliminate dangerous conditions. NOTE: This must be a continuing effort and a consideration in the assignment of security management responsibilities. The security inspection plan should include verification of compliance with established standards.

Fire Detection

Despite careful attention to the location, design, construction, and operation of the AIS facility, there is still the possibility of a fire. Experience shows repeatedly that prompt detection is a major factor in limiting fire damage. Typically, a fire goes through three stages. Some event, such as a failure of electrical insulation, causes ignition. An electrical fire will often smolder for a long period of time. When an open flame develops, the fire spreads through direct flame contact, progressing relatively slowly, with a rise in the temperature of the surrounding air. The duration of this stage is dependent on the combustibility of the materials at and near the point of ignition. Finally, the temperature reaches the point at which adjacent combustible materials give off flammable gases. At this point, the fire spreads rapidly and ignition of nearby materials will result from heat radiation as well as direct flame contact. Because of the high temperatures and volumes of smoke and toxic gases associated with this third stage, fire fighting becomes increasingly difficult and often prevents people from remaining at the fire site.

Given the objective to discover and deal with a fire before it reaches the third stage, one can see the limitation of fire detection that depends on detecting a rise in air temperature. For this reason, the areas in which electronic equipment is installed should be equipped with products-of-combustion (smoke) detectors. Such detectors use electronic circuitry to detect the presence of abnormal constituents in the air that are usually associated with combustion.

In designing an effective fire detection system, consider the following points:

- **Location and spacing of detectors.** The location and spacing of detectors should take into consideration the direction and velocity of air flow, the presence of areas with stagnant air, and the location of equipment and other potential fire sites. Note that detectors may be required under the raised floor, above the hung ceiling, and in air-conditioning ducts as well as at the ceiling. It may also be wise to put detectors in electric and telephone equipment closets and cable tunnels.
- **Control panel design.** The design of the detection control panel should make it easy to identify the detector that has alarmed. This implies that the detectors in definable areas (for example, the tape vault, the east end of the

computer room, and administrative offices) should be displayed as a group on the control panel. In other words, when an alarm sounds, inspection of the control panel should indicate which area or zone caused the alarm. Generally, and preferably, each detector includes a pilot light that lights when the detector is in the alarm state. In some cases there should be a separate indicator light at the control panel for each detector. It is also important to see that the alarm system itself is secure. Its design should cause a trouble alarm to sound if any portion of it fails, or if there is a power failure. Take steps to assure the system cannot be deactivated readily, either maliciously or accidentally.

- **Personnel response.** Meaningful human response to the detection and alarm systems is necessary if they are to be of any value. This means the fire detection system should be designed to assure that someone will always be alerted to the fire. Typically, the computer room staff is expected to respond to an alarm from the AIS facility alarm system. A remote alarm should also be located at another point in the building that is occupied at all times, such as the lobby guard post, security center, or building engineer's station. This provides a backup response when the computer area is not occupied. If there is any possibility the remote alarm point will not be occupied at all times, a third alarm point should be located offsite, usually at the nearest fire station or the command's fire department for the facility.
- **Maintenance.** Proper maintenance is essential to the fire detection system. The nature of smoke detectors is such that nuisance alarms may be caused by dust in the air or other factors. Because of this, there is a tendency to reduce sensitivity of the detectors to eliminate nuisance alarms, with the result that detection of an actual fire may be delayed. To ensure proper operation, see that qualified personnel (a vendor representative, building engineer, or Public Works Center personnel) verify correct operation at the time of installation, and at least once each year thereafter. Furthermore, each fault condition should be corrected immediately. Unfortunately, a common tendency is to turn off the fire detection system or silence the alarm bell, creating the danger that there will be no response if a fire should occur.

In addition to alerting personnel to the presence of a fire, the detection equipment can be used to control the air-conditioning system. There is some support for the view that, upon detection, air-handling equipment be shutdown automatically to avoid fanning the flames and spreading smoke. This is not the best plan, as nuisance alarms will result in needless disruption. The preferred technique is to cause the system to exhaust smoke by stopping recirculation, and switching to 100-percent outside air intake and room air discharge. As a rule, this can be done by adjusting air-conditioning damper controls and their interconnection with the fire detection system. However, it may be necessary to modify the air-conditioning system. The use of either technique is at the discretion of command policy.

Fire Extinguishment

Fire extinguishment may be accomplished using one or more of the following four methods:

- **Portable or hand extinguishers.** Operated by military or civil service personnel to help control the fire before it gets out of hand.
- **Hose lines.** Used by military, civil service, or professional fire fighters to attack the fire with water.
- **Automatic sprinkler systems.** Release water from sprinkler heads activated in the temperature range of 135°F to 280°F.
- **Volume extinguishment systems.** Fill the room with a gas that interferes with the combustion process.

To ensure the effectiveness of portable extinguishers, several measures should be observed. Place extinguishers in readily accessible locations, not in corners or behind equipment. Mark each location for rapid identification; for example, paint a large red spot or band on the wall or around the column above the point where each extinguisher is mounted. It is important for each AIS technical manager to ensure proper inspection in accordance with command policy. Each extinguisher should have an inspection tag affixed to it with the signature of the inspecting petty officer or fire marshal and the inspection date.

In all probability, the AIS facility technical manager will want to establish a first line of defense against fire involvement between the time of notification of, and response by, professional or highly trained firefighters, and will incorporate this as part of the command's Disaster Control Plan. Every command, regardless of

size, needs military personnel who are knowledgeable and trained in fire safety. Any practical and effective organization for fire protection must be designed to assure prompt action immediately at the point where a fire breaks out. This usually necessitates every organizational unit or area of a command having a nucleus of key personnel who are prepared, through instruction and training, to extinguish fires promptly in their beginning stage. Such individuals become knowledgeable in specialized fire protection and the systems applicable to the facility in question: how to turn in an alarm, which type of extinguisher to use for which type of fire, and how to use it. Further, such individuals can serve as on-the-job fire inspectors, constantly seeking out, reporting, and correcting conditions that may cause fires. They can help ensure that fire-fighting equipment is properly located and maintained, that storage does not cause congestion that could hamper fire fighting, and that general housekeeping is maintained at a reasonably high level to minimize fire risk.

SUPPORTING UTILITIES PROTECTION

Every Navy AIS facility is dependent upon supporting utilities, such as electric power and air conditioning, and may have to depend on communication circuits, water supplies, and elevators for its operation. Not all commands are self-sufficient; they contract some or all of these utilities from civil sources. In using these utilities, AIS technical managers should consider the probability of occurrence and the effects of breakdowns, sabotage, vandalism, fire, and flooding. These effects can then be related to the needs of the AIS facility as established by the risk analysis.

We have selected electrical power to illustrate support utility protection. Variations of a normal waveform in the electric power supply can affect the operation of AIS hardware. The AIS hardware rectifies the alternating current, filters, and voltage; regulates the resulting direct current; and applies it to the AIS circuitry. The filtering and regulation cannot be expected to eliminate voltage variations beyond a reasonable range. If line voltage is 90 percent or less of nominal for more than 4 milliseconds, or 120 percent or more of nominal for more than 16 milliseconds, excessive fluctuations can be expected in the dc voltage applied to the hardware circuitry. This power fluctuation causes unpredictable results on hardware, logic, and data transfer. These power line fluctuations, referred to as *transients*, are usually caused by inclement weather.

Internally generated transients depend on the configuration of power distribution inside the AIS facility. The effects of internal transients can be minimized by isolating the AIS hardware from other facility loads. Ideally, the computer area power distribution panels should be connected directly to the primary feeders and should not share step-down transformers with other high-load equipment.

The risk analysis should include a complete power transient and failure study. It should also carefully consider the projected growth in particularly sensitive applications (such as real-time or teleprocessing) in projecting future loss potential.

In some cases it may be economically feasible to connect the AIS facility to more than one utility feeder via a transfer switch. If one feeder fails, the facility's load may be transferred to the alternate feeder. This technique is of greater value if the two feeders connect to different power substations.

If the AIS facility is in a remote area, an uninterrupted power supply (UPS) is usually required as a backup power source. The UPS system can be manually or automatically controlled from prime power sources or from the AIS computer site. The typical UPS consists of a solid-state rectifier that keeps batteries charged and drives a solid-state inverter. The inverter synthesizes alternating current for the computer. A simplified block diagram is shown in figure 4-8.

Depending on the ampere-hour capacity of the battery (or batteries), the UPS can support its load for a maximum of 45 minutes without the prime power source. At the same time, it will filter out transients. To provide extra capacity to protect against a failure of the UPS, a static transfer switch can be inserted between the UPS and the computer, as shown in figure 4-9. The control circuitry for the static switch can sense an overcurrent condition and switch the load to the prime power source without causing noticeable transients.

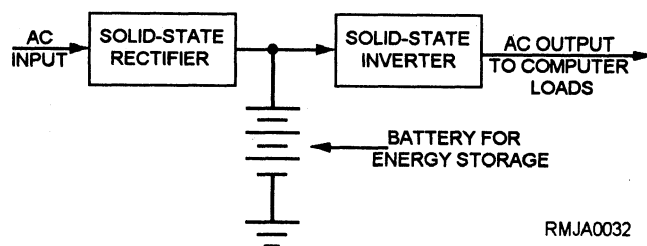


Figure 4-8.—Simplified block diagram of an uninterruptible power supply (UPS).

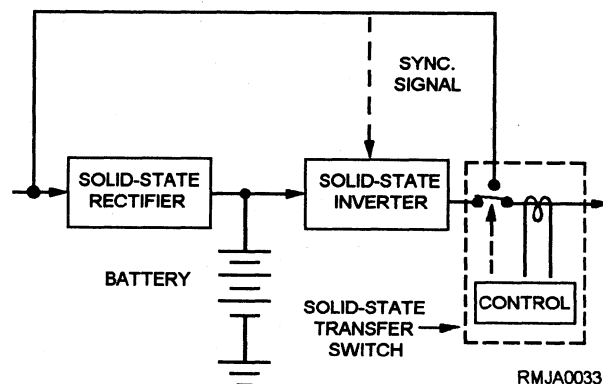


Figure 4-9.—UPS with transfer switch.

If the facility's current needs exceed its UPS capacity, it may be economically feasible to use multiple, independent UPS units, as shown in figure 4-10. Since each unit has its own disconnect switch, it can be switched offline if it fails.

Finally, if the risk analysis shows a major loss from power outages lasting 30 to 45 minutes or beyond, an onsite generator can be installed, as shown in figure 4-11. The prime mover may be a diesel motor or a turbine. When the external power fails, UPS takes over and the control unit starts the prime mover automatically. The prime mover brings the generator up to speed. At this point, the UPS switches over to the generator. Barring hardware failures, the system supports the connected load as long as there is fuel for the prime mover. Note that the generator must be large enough to support other essential loads, such as air conditioning or minimum lighting, as well as the UPS load.

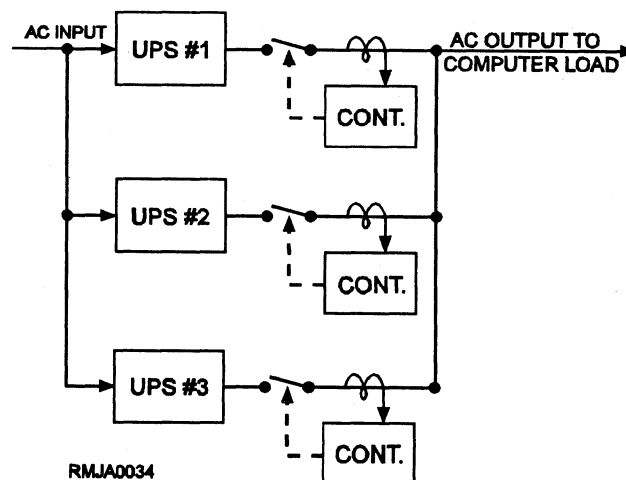


Figure 4-10.—Multiple, independent UPS units.

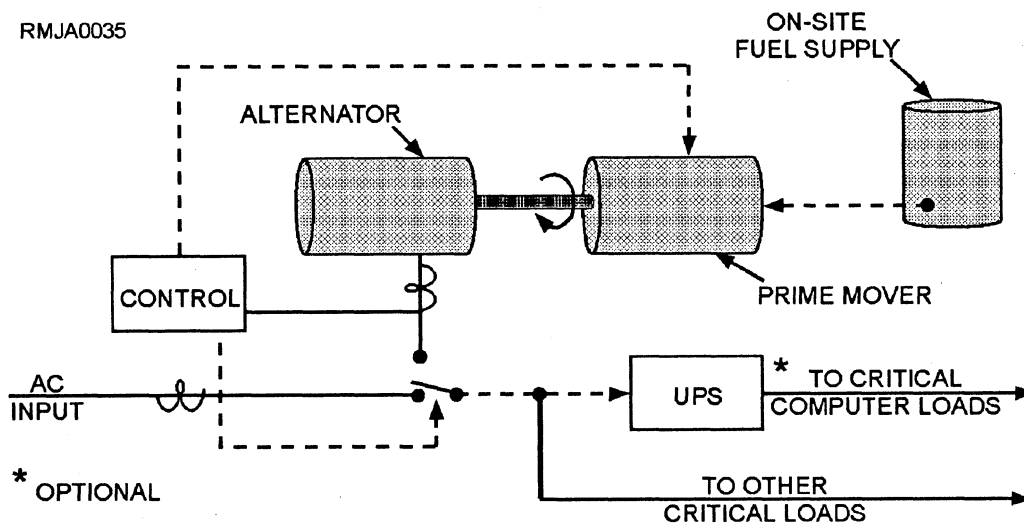


Figure 4-11.—UPS with onsite generation.

When this configuration is used, maintain a close communication liaison with the power plant source to ensure the generator is coming up to normal speed for the switchover from UPS. The UPS system takes over automatically, and the change in power source may not be noticed in the AIS facility. However, when the UPS system changes over to the generator, it may require a manual power panel setting in the AIS facility by the AIS technical manager.

AIS FACILITY PHYSICAL PROTECTION

The physical protection of the AIS facility can be thought of as the process of permitting access to the facility by authorized persons, while denying access to others. The physical protection of an AIS facility is not as stringent for an AIS facility that processes unclassified data as it is for an AIS facility that processes classified data. In the following example/discussion, assume the facility processes classified material and provides physical protection in accordance with OPNAVINST 5510.1 and OPNAVINST 5530.14. Pay particular attention to applying physical protection and security policy wherever AIS equipment is used for processing classified information in accordance with OPNAVINST 5239.1.

Ensure plans are developed for the protection, removal, or destruction of classified material in the case of a natural disaster, civil disturbance, or enemy action. The plans should establish detailed procedures and responsibilities for the protection of classified material so that it does not fall into unauthorized hands in the event of an emergency. Also, indicate what material is to be guarded, removed, or destroyed. An adequate emergency plan for classified material should provide for guarding the material, removing the classified

material from the area, complete destruction of the classified material on a phased priority basis, or appropriate combinations of these actions.

The emergency plans should also provide for the protection of classified information in a manner that minimizes the risk of loss of life or injury to AIS personnel. The immediate placement of a trained and preinstructed perimeter guard force around the affected area to prevent the removal of classified material is an acceptable means of protecting the classified material. This action reduces the risk of casualties.

Security requirements for the central computer AIS facility area should be commensurate with the highest classified and most restrictive category of information being handled in the AIS. If two or more computer systems are located in the same controlled area, the equipment comprising each system may be located so that direct personnel access, if appropriate, is limited to a specific system.

Boundary Protection

The threat analysis may indicate the need to protect the property boundary of the AIS facility. This may be accomplished by installing fences or other physical barriers, outside lighting, or perimeter intrusion detectors, or by using a patrol force. Often a combination of two or more of these will be sufficient. Fences should be 8 feet high with three strands of barbed wire. Fences provide crowd control, deter casual trespassers, and help in controlling access to the entrances; however, they do not stop the determined intruder.

In situations where manpower shortages exist, the fence can be equipped with penetration sensors that should sound an internal alarm only. This type of

physical protection system uses small sensors mounted at intervals on the fence and at each gate.

Emanations Protection

In evaluating the need for perimeter protection, take into account the possibility that electromagnetic or acoustic emanations from AIS hardware may be intercepted. Tests show that interception and interpretation of such emanations may be possible under the right conditions by technically qualified persons using generally available hardware. As a rule of thumb, interception of electromagnetic emanations beyond 325 yards is very difficult. However, if there is reason to believe that a potential exposure to interception exists, seek technical guidance from upper management and the Chief of Naval Operations.

Measures to control compromising emanations are subject to approval under the provisions of *Control of Compromising Emanations*, DOD Directive C5200.19, by the cognizant authority of the component approving security features of the AIS system. Application of these measures within industrial AIS systems is only at the direction of the contracting activity concerned under provisions of the *Security Requirements for Automated Information Systems (AIS's)*, DOD Directive 5200.28, and the requirements are to be included in the contract.

Interior Physical Protection

Intrusion detection systems (IDSs) (OPNAVINST 5510.1) provide a means of detecting and announcing proximity or intrusion that endangers or may endanger the security of a command. The use of an IDS in the protective program of a command may be required because of the critical importance of a facility or because of the location or the layout of the command.

Remember, IDSs are designed to detect, not prevent, an attempted intrusion. Thus, a comprehensive security plan must contain appropriate security measures along with procedures for an effective reaction force.

Remote Terminal Areas Protection

The physical and personnel security requirements for the central computer facility area are based upon the overall requirements of the total AIS system. The remote terminal area requirements are based upon the highest classified and most restrictive category and type of material that will be accessed through the terminal under system constraints.

Each remote terminal should be individually identified to ensure required security control and

protection. Identify each terminal as a feature of hardware in combination with the operating system.

Before personnel of a component that is not responsible for the overall AIS operation can use a remote device approved for handling classified material, security measures must be established. These security measures are established by the authority responsible for the security of the overall AIS. They are agreed to and implemented before the remote device is connected to the AIS.

DOD component systems may become part of a larger AIS network. The approval and authority to authorize temporary exceptions to security measures for the component's system in the network requires two components. These include the DOD component operating the AIS system and the DOD component having overall responsibility for the security of the network.

Each remote terminal that is not controlled and protected as required for material accessible through it should be disconnected from the AIS system when the system contains classified information. Disconnect procedures are used to disconnect remote input/output terminals and peripheral devices from the system by a hardware or software method authorized by the designated approving authority of the central computer facility.

Security Survey

An annual security survey of the AIS facility area should be conducted by the AIS technical manager. The first step of the survey is to evaluate all potential threats to the AIS facility as discussed earlier in this chapter. The second step is to define and tabulate areas within the facility for control purposes. Details depend on the specifics of each facility, but the following are common areas to consider:

- Public entrance or lobby;
- Loading dock;
- Spaces occupied by other building tenants;
- AIS facility reception area;
- AIS input/output counter area;
- AIS data conversion area;
- Media library;
- Systems analysis and programming areas;
- Computer room spaces;

- Communications equipment spaces; and
- Air conditioning, UPS, and other mechanical or electrical equipment spaces.

The survey should verify security measures already in place and recommend any improvements to upper management. Obtain a current floor plan on which to depict all areas within the facility. Include all access points and any adjacent areas belonging to the AIS facility, such as parking lots and storage areas. Begin the survey at the perimeter of the AIS facility, considering the following:

- **Property line.** Include fencing, if any, and type. Note the condition, the number of openings according to type and use, and how they are secured. Are there any manned posts at the property line?
- **Outside parking facilities.** Are these areas enclosed, and are there any controls? Are parking lots controlled by manned posts or are devices used?
- **Perimeter of facility.** Note all vehicular and pedestrian entrances and what controls are used, if any. Check all doors—their number, how they are secured, and any controls or devices, such as alarms or key card devices. Check for all ground floor or basement windows and how they are secured, screening or bars, for example, and their vulnerability. Check for other entrances, such as vents and manholes. Are they secured and how? Check for fire escapes—their number and locations and accessibility to the interior of the facility from the fire escape (windows, doors, roof). How are accessways secured?
- **Internal security.** Begin at the top floor or in the basement. Check for fire alarm systems and devices. Note the type, location, and number. Where does the alarm annunciate? Check telephone and electrical closets to see if they are locked. Are mechanical and electrical rooms locked or secured? Note any existing alarms as to type and number. Determine the number and locations of manned posts, hours, and shifts.
- **Monitoring facility.** Know the location, who monitors, who responds, its type, and the number of alarms being monitored.

Table 4-6 is a checklist of other questions that should be asked in the survey.

Table 4-6.—Security Measures Checklist

No.	Security Measure	Status
1.	Is the facility/building protected by (an) alarm system(s)?	
2.	How many zones of protection are within the protected building?	
3.	Is the alarm system adequate and does it provide the level of protection required?	
4.	Are there any vulnerable areas, perimeter, or openings not covered by an alarm system?	
5.	Is there a particular system that has a high nuisance alarm rate?	
6.	Is the alarm system inspected and tested occasionally to ensure operation?	
7.	Is the system backed up by properly trained, alert protection personnel who know what steps to take in case of an alarm?	
8.	Is the alarm system regularly inspected for physical and mechanical deterioration?	
9.	Does the system have tamper-proof switches to protect its integrity?	
10.	Is there an environmental or protective housing or cover on the system(s)?	
11.	Is there an alternate or separate source of power available for use on the system in the event of an external power failure?	
12.	Where is the annunciating unit located—local, central station, or remote?	
13.	Who maintains the equipment and how is it maintained (contract, lease equipment, force account personnel, military, or civil service)?	
14.	Is the present equipment up-to-date?	
15.	Are records kept of all alarm signals received, including the time, date, location, action taken, and cause of the alarm?	
16.	Are alarms generated occasionally to determine the sensitivity and the capabilities of systems?	

When the security survey is complete, it provides a picture of the existing alarm systems and the location of each. It also shows the number and location of manned posts, the number of personnel at these posts, and the schedule of each.

With these facts in hand, the AIS technical manager can evaluate existing access controls and protection measures, identify areas where remedial measures are needed, and select specific measures.

Always consider the use of various types of security hardware devices to augment the existing personnel protective force. Through the use of such devices, it may be possible to save on operating cost.

CONTINGENCY PLANNING

Operation plans and the command's organizational manual are prepared and executed for the accomplishment of the command's specific mission. These operation plans assume normal working conditions, the availability of command resources and personnel, and a normal working atmosphere. Despite careful use of preventive measures, there is always some likelihood that events will occur that could prevent normal operations and interfere with the command accomplishing its mission. For this reason, contingency plans are included in the AIS security program. For the purpose of this chapter, we refer to these contingency plans as the Continuity of Operations Plan (COOP).

Three different types of contingency plans makeup a COOP security program for an AIS facility:

- **Emergency response.** There should be procedures for response to emergencies, such as fire, flood, civil commotion, natural disasters, bomb threats, and enemy attack, to protect lives, limit the damage to naval property, and minimize the impact on AIS operations.
- **Backup operations.** Backup operation plans are prepared to ensure essential tasks (as identified by the risk analysis) can be completed subsequent to disruption of the AIS and that operations continue until the facility is sufficiently restored or completely relocated.
- **Recovery.** Recovery plans should be made to permit smooth, rapid restoration of the AIS facility following physical destruction or major damage.

Each AIS facility should establish and appoint members to a formal board to construct, review, and recommend command procedures for approval in creating a COOP program. Figure 4-12 shows suggested tasks and how they may be set up and assigned. Each AIS facility will need to adapt to its own special circumstances and make full use of the resources available to it.

EMERGENCY RESPONSE PLANNING

The term *emergency response planning* is used here to refer to steps taken immediately after an emergency occurs to protect life and property and to minimize the impact of the emergency. The risk analysis should be reviewed by the AIS technical manager to identify emergency conditions that have particular implications for AIS operations, such as protection of equipment during a period of civil commotion and subsequent to a natural disaster (fire or flood, for example). Where civil commotion and natural disaster are found, local instructions should be developed and implemented to meet the special needs of the AIS facility. These instructions and procedures may be designated the "Loss Control Plan" and implemented as part of COOP.

Loss control can be particularly important to the AIS facility. In a number of recent fires and floods, the value of being prepared to limit damage is amply demonstrated. By reviewing operations and the locations of critical equipment and records with shift leaders, the AIS technical manager can develop measures to use in case of an emergency. The guidelines should be similar to the following:

1. Notify online users of the service interruption.
2. Terminate jobs in progress.
3. Rewind and demount magnetic tapes; remove disk packs.
4. Power down AIS hardware and cover with plastic sheeting or other waterproof material.
5. Put tapes, disks, run books, and source documents in a safe place.
6. Power down air-conditioning equipment.

If evacuation of work areas is ordered or likely, instruct all personnel to:

	COOP BOARD MEMBERS						
	AIS Technical Manager	User Representatives	CO XO GS	Upper Management	Security Officer	Supply Division	Public Works Center
1. Establish board members	*			*			*
2. Estimate recovery time	*					*	*
3. Failure mode analysis							
AIS hardware	*						*
Utility failure	*				*		*
Fire, flood, wind	*				*		*
4. Loss potential	*	*		*			*
5. Emergency response plans	*			*	*		*
6. Selection of backup modes	*	*		*			*
7. Recovery plans	*	*		*		*	*

Figure 4-12.—Organization and tasks for COOP.

1. Put working papers and other unclassified material in desks or file cabinets and close them.
2. Turn off equipment, but leave room lights on.
3. Close doors as areas are evacuated, but ensure that locks and bolts are not secured.

The loss control plan should define the steps to be taken, assign responsibilities for general and specific steps, and provide any needed materials and equipment in handy locations. In some cases, ample time will be available to take all measures, but in extreme emergencies, life safety will dictate immediate evacuation. For this reason, the loss control plan should

designate one or more individuals in each AIS area who, in the event of an emergency, will determine what can be done to protect equipment and records without endangering life, and direct AIS staff members accordingly.

Earlier in this chapter, we discussed measures to protect the facility against the effects of fire. Semiannually, review the protective plans with the operations division officer to assure that all normal requirements and any special requirements of the AIS facilities are satisfied. At the same time, brief upper management on the AIS facility plans and status, to get their advice and to ensure good coordination.

When emergency response planning is completed and approved, it should be documented succinctly for easy execution. See figure 4-13.

COOP BACKUP PLANNING

The risk analysis should identify those situations in which backup operations will probably be needed to avoid costly delays in accomplishing the command mission. The next step is to develop plans for backup operations, which are economically, technically, and operationally sound. Details will depend on circumstances at the AIS facility, but some general guidance and suggestions can be helpful in considering the alternatives.

Backup operations may take place onsite when there is only a partial loss of capability. However, they may require one or more offsite locations when there is major damage or destruction. The backup procedures may replicate normal operation or be quite different. When considering backup, AIS management will often find that an exact replica of the onsite AIS system is not available for backup or the time available per day is less than the amount needed to complete all assigned tasks. From this, you might conclude that backup is impossible. On the contrary, a number of things can be done to make backup resources available. The following are examples:

- **Postpone the less urgent tasks.** Tabulate the AIS tasks in descending order of urgency as identified by the risk analysis. Having estimated the time to return to normal following a disruptive event, AIS management can quickly see which tasks can be set aside. These include such things as program development, long cycle (monthly, quarterly, or annual) processing, and long-range planning. As long as adequate catch-up time is available after the return to normal, there should be a number of tasks that can be safely postponed.

FIRE EMERGENCY RESPONSE

1. Report fire (list phone number).
2. Assess life-safety hazard.
3. Evacuate facility if necessary.
4. Initiate loss control procedures.

Figure 4-13.—Fire emergency response.

- **Substitute other procedures.** If increased cost or degraded service can be accepted temporarily, it may be possible to use other procedures. If printer capability is lost, print tapes could be carried to a backup facility for offline printing. It might also be possible to substitute batch processing for online processing temporarily. In some cases, where compatible hardware is not available, it may be feasible to maintain a second software package that is functionally identical to the regular package but technically compatible with the offsite AIS hardware that is available for backup use.
- **Modify tasks to reduce run time.** To stretch available backup resources, it might be feasible to eliminate or postpone portions of a task, such as information-only reports or file updates that are not time urgent. In some cases, it might help to double the cycle time for a task; that is, run a daily task every other day instead.

By considering these possibilities for each task, the AIS technical manager can develop the specifications for the minimum backup requirements (AIS hardware, resources, and hours per day necessary for adequate backup).

To evaluate alternate backup modes and offsite facilities, consider such factors as:

- AIS hardware usage;
- Transportation of military and civil service personnel with needed supplies and materials;
- Maintenance personnel at the offsite location; and
- Overtime cost factor for civil service personnel.

As these factors come into focus—identification of critical tasks, specific backup modes, and usable offsite AIS facilities—the outlines of the optimum backup plan will begin to emerge. In general, it is wise to form several COOP backup plans; for example:

- **A minimum duration plan.** A plan for backup operation that is not expected to extend much beyond the cause of delay which forces a shift to backup operation; namely, a minimum duration plan that would probably include only the most time urgent AIS tasks.
- **A worst-case plan.** A plan for backup operation for as long as it takes to reconstruct the AIS facility after total destruction.

- **In-between plans.** Plans for one or more operating periods between minimum duration and worst case.
- **A plan for each major partial failure mode.**

While the individual COOP plans are geared to different objectives, they can usually be constructed from a common set of modules. It is often most effective to make a detailed plan for total destruction since this is the most demanding situation. Scaled-down versions or individual elements from this plan can then be used for the less-demanding situations.

Each COOP backup plan should cover the following five basic areas:

- **Performance specifications.** This is a statement of the specific ways in which performance of each task departs from normal; for example, tasks postponed, changes in cycle times, and schedules.
- **User instructions.** Backup operation may require users to submit input in different forms or to different locations or may otherwise call for altered procedures. These should be clearly spelled out to avoid confusion and wasted motion.
- **Technical requirements for each AIS task.** Backup operation of an AIS task will require the availability at the offsite AIS facility of the following items: current program and data files, input data, data control and operating instruction (which may differ from normal instruction), preprinted forms, carriage control tapes, and the like. These requirements must be documented for each task. Procedures also need to be established to ensure the materials needed for backup operation are maintained offsite on a current basis.
- **Computer system specifications.** One or more offsite computer systems are selected for backup operation. The following information should be recorded for each system: administrative information about the terms of backup use, the location of the system, the configuration and software operating system, a schedule of availability for backup operation, and the tentative schedule of AIS tasks to be performed on the system.

- **Administrative information.** It is probable that COOP backup operation will require special personnel assignments and procedures, temporary employment or reassignment of personnel, use of special messengers, and other departures from normal. Details are to be documented, along with guidance on obtaining required approvals.

When each of the COOP backup plans is completed, it should include full documentation and have upper management approval. Each of the plans may have considerable duplication. However, it is suggested that each plan be completely documented to be sure nothing has been overlooked.

RECOVERY PLANNING

The use of a backup facility usually means both extra expense and degraded performance. Therefore, give some thought to recovery by developing and maintaining supporting documents that minimize the time required for recovery. Furthermore, the AIS staff will be hard pressed by backup operations. If others can handle recovery, the workload on the AIS staff will be reduced during the emergency and the process will undoubtedly be carried out more effectively and economically. Recovery from total destruction requires the following tasks be completed:

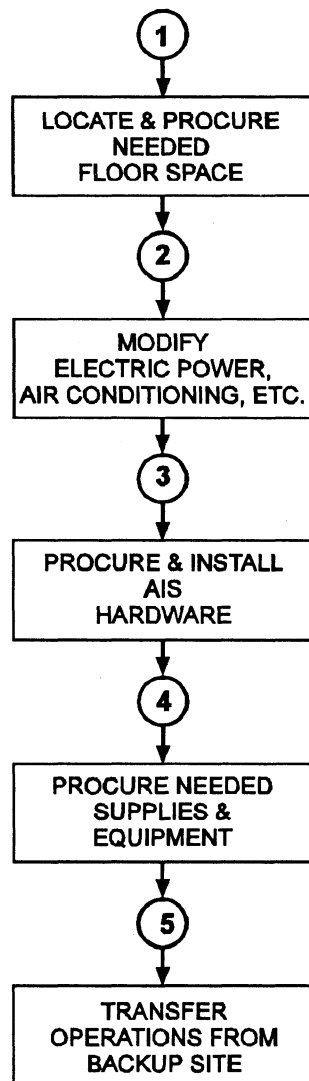
- Locate and obtain possession of enough floor space to house the AIS facility with a live-load capacity as required by the AIS hardware and suitably located with respect to users and AIS staff spaces.
- Perform required modifications for needed partitions, raised floor, electric power distribution, air conditioning, communications, security, fire safety, and any other special requirements.
- Procure and install AIS hardware.
- Procure needed supplies, office equipment and furniture, tape storage racks, decollators, and so forth.
- Verify that all needed hardware, equipment, and materials are on hand and in good working order. Then transfer operations from the backup site to the reconstituted AIS facility.

If the necessary documents have been prepared and stored offsite before the emergency, it should be possible for all but the last tasks to be completely

reconstructed with minimum effort. Figure 4-14 shows a simplified step diagram of a normal reconstruction effort.

COOP TESTING

Because emergencies do not occur often, it is difficult to assure adequacy and proficiency of personnel and plans without regular training and testing. Therefore, it is important to plan and budget for both. The availability of needed backup files may be tested by attempting to repeat a particular task using onsite hardware but drawing everything else from the offsite location. Experience demonstrates the value of such tests in validating backup provisions; it is not uncommon to discover gross deficiencies despite the most careful planning. Compatibility with the offsite facility should be verified regularly by running one or more actual tasks. A number of AIS facilities conduct such tests as a part of an overall inspection.



RMJA0037

Figure 4-14.—Simplified diagram of an AIS facility

Similar tests of procedures for fire fighting, loss control, evacuation, bomb threat, and other emergencies will give assurance that plans are adequate and workable. At the same time, they provide an opportunity for training AIS personnel. Each test should have a specific objective. A team should be assembled to prepare a scenario for the test, to control and observe the test, and to evaluate the results. This evaluation provides guidance for modifications to emergency plans and for additional training. The important point is to be sure the emergency plans do, in fact, contribute to the security of the AIS facility.

SECURITY INSPECTIONS

The final element of the AIS security program for every naval AIS facility should be a review or inspection process. The inspection should be an independent and objective examination of the information system and its use (including organizational components) and including the following checks:

- Checks to determine the adequacy of controls, levels of risks, exposures, and compliance with standards and procedures; and
- Checks to determine the adequacy and effectiveness of system controls versus dishonesty, inefficiency, and security vulnerabilities.

The words *independent* and *objective* imply the inspection complements normal management inspections, visibility, and reporting systems and is neither a part of, nor a substitute for, any level of management.

What can an inspection be expected to accomplish? First, it evaluates security controls for the AIS facility. Second, it provides each level of management an opportunity to improve and update its security program. Third, it provides the impetus to keep workers and management from becoming complacent. Fourth, if done effectively, it tends to uncover areas of vulnerability. Remember, risks change, and new threats arise as systems mature.

Major factors to consider in determining the frequency of internal inspections include the frequency of external inspections, the rate of change of the AIS, the amount and adequacy of controls, the threats that face the facility, the results of previous inspections, and the directions of higher authority. Inspection activity, direction, and implementation are usually at the discretion of the commanding officer of the command with jurisdiction over the AIS facility.

INSPECTION PREPARATION

The inspection should be conducted by some department or facility outside the span of control of the AIS technical manager. One of the main principles in selecting an inspection team is that members should not be responsible for AIS operations. Team members should have some knowledge of data processing and, if possible, basic inspection principles. A programming or AIS operations background is desirable but not essential. An experienced military or civil service user of AIS services might have the necessary qualifications. The role of the team is not to develop security controls, but to evaluate established controls and procedures. Also, the team should not be responsible for enforcing control procedures, which is clearly an AIS management responsibility.

The character of each of the inspection team members is extremely important. Judgment, objectivity, maturity, ability, and a probing nature will all affect the success of the inspection. The leader of the inspection team must be able to organize the efforts, prepare a good written report, and communicate findings effectively. The leader should be an officer, warrant officer, chief petty officer, or U.S. civilian employee who is GS-7 or above. If not technically oriented, the team leader should be assisted by someone whose technical judgment and knowledge of AIS is reliable.

The size of the team depends upon the size of the facility and the scope of the inspection. A large facility should consider including personnel from the following areas on the inspection team:

- **Internal inspection.** The knowledge and discipline to conduct an inspection can be provided through internal inspection specialists. Inquisitiveness, a probing nature, and attention to detail are typical characteristics desired for inspection board members. Even though an inspection team member generally is not trained in data processing technology, it should not be difficult to appoint team members with some data processing knowledge.
- **Security.** A security officer is a welcome addition to an inspection team.
- **Computer operations.** Technical expertise in data processing is required. Both programming knowledge and operations experience is helpful. Perhaps the data processing internal security officer has these skills and, if so, should be a prime candidate for the team. Using someone

from the AIS facility being evaluated need not significantly affect the objectivity of the inspection process.

- **Users.** Users have the most to gain from an effective inspection because of their dependence on the AIS facility, yet too often they have little or no interest in AIS controls or security measures. To encourage participation in the AIS security program, one or more users who are concerned about sensitive data being compromised, disclosed, or destroyed should be motivated to join or should be appointed to the inspection team.
- **Building management.** Many of the physical security controls to be inspected—fire prevention and detection, air conditioning, electric power, access controls, and disaster prevention—relate to building management and engineering.
- **Outside specialists.** Independent, experienced viewpoints provided by outside consultants can be very helpful.

The composition of the team can be flexible. One of the prime requirements is that it consist of people who are objective. If only one AIS facility is to be inspected, the members of the team can be assigned for the term of the inspection and then returned to their normal jobs. If there are many AIS facilities under the jurisdiction of the command, it might be advisable to establish a permanent inspection team to review all facilities on a recurring basis. In any event, the composition of the team should be changed periodically to bring in fresh viewpoints and new and different inspection techniques.

THE INSPECTION PLAN

A comprehensive inspection plan must be developed to properly conduct an internal inspection of security. It should be action-oriented, listing actions to be performed. The plan must be tailored to the particular facility. It should include the report and report formatting requirement and the distribution of the final report. This means quite a bit of work is required in its development.

The first step is to examine the security policy for the AIS facility. This policy may apply to an entire naval district, a command, a ship, a department, or a single AIS facility. In any case, the security policy should be reviewed and pertinent security objectives extracted for subsequent investigation. The next step is to review the risk analysis plan, identifying those

vulnerabilities that are significant for the particular facility. Third, the AIS Facility Security Manual, the Operations Manual, and other appropriate documents should be reviewed to determine what the specified security operating procedures are. And last, the AIS facility organization chart and job descriptions should be examined to identify positions with specific security or internal control responsibilities. This background material forms the basis for the development of the inspection plan. A number of general questions should be considered when formulating the inspection program. The following are examples:

- **What are the critical issues with regard to security?** Does the AIS facility process classified or otherwise sensitive data? Does the processing duplicate that of other data centers, thereby providing some sort of backup or contingency capability? Or is it a stand-alone activity processing unique applications? What are the critical applications in terms of the inspection emphasis?
- **What measures are least tested in day-to-day operations?** For example, if the computer fails every day at 1615 because of power switchovers, the immediate backup and recovery requirements are likely to be well formulated and tested. However, the complete disaster recovery plan probably has not been tested, unless there is a specific policy to do so. This is a key point. Security measures of this type are often inadequately exercised.
- **What inspection activities produce the maximum results for least effort?** A test of fire detection sensors under surprise conditions tests not only the response to alarms but also the reaction of the fire party and the effectiveness of evacuation plans. In interviewing personnel, the team should design questions to elicit comprehensive answers. For example, the question "How would you process an unauthorized job?" is likely to elicit more information than "Are job authorization controls effective?" The most likely answer to the second question is a simple and uninformative "Yes."
- **What are the security priorities?** Because of particular policy, a request for an investigation, or an incident of loss, interruption, or compromise, the testing of a particular security measure probably should receive more emphasis than another equally important but noncurrent

topics. One must, however, avoid irrational concentration on anyone aspect of the program. Management overemphasis as a result of a recent security breach should be tempered with a rational approach toward investigating all aspects of computer security.

Another step in the process of developing an inspection plan is the review of previous inspection reports. Many times these identify weaknesses or concerns that should have been corrected, and so should be an item of special attention in the current inspection.

CONDUCTING INSPECTIONS

Advantages can be gained from using both scheduled and surprise inspections. A scheduled inspection should meet the general policy requirements of the particular facility and should occur at least annually. This could be a major inspection conducted by an outside command, an internal inspection, or a spot check inspection to review specialized items of interest, perhaps as a result of previous inspection reports of findings. The distinguishing characteristic is that it is scheduled in advance, with a resultant flurry of preparation by the AIS facilities. It motivates cleaning up loose ends, but limits what can really be learned from the inspection.

A surprise inspection is designed to test on a no-notice basis certain elements of security and control. It should be approved by the commanding officer of the command in charge of the AIS facility. It can be accomplished by the command or an external inspection team. It can be used to test those elements best reviewed on a surprise basis, such as fire response, access control, and personnel complacency.

When a scheduled inspection is conducted, the first step normally is to interview AIS personnel. Generally, the first walk-through includes interviews with the AIS technical manager. Searching questions, rather than leading questions, should be the rule, and the best approach is to allow the interviewee to talk as freely as possible. If you are the interviewer, ask questions to put the interviewees in the position of probing for their answers. For example, "What is your biggest access control problem?" not "Do your people wear badges?" Ask how illegal entry or sabotage would be accomplished. Do not hesitate to ask the same questions of more than one person. It is interesting how varied the responses can be.

The conduct of the interviewer is important. Strive to be open in dealing with interviewees. Avoid allusions to private information and obscure references

to other people or events or in any other way cultivating an air of mystery or superiority. It goes without saying the use of good human relations techniques is essential to a successful interview. Nothing can be gained by being belligerent and antagonizing the interviewee. Your conduct should be firm and inquisitive, but also calm, sincere, and open. Probe in some detail any answer that appears evasive or defensive.

Taking notes is a matter of individual preference. Some people take very adequate notes at listening speed. Others must devote all their attention to listening. If note taking is a problem, the interview could be conducted by two-person teams. Another alternative is to use a portable tape recorder, making certain the interviewee knows in advance that the interview is being taped. If a two-person team or a tape recorder is not available, attempt to listen and absorb as much as possible, then record notes and impressions directly after the conclusion of the interview.

The evaluation tests can be scheduled or come as a surprise. Most security inspections include testing the emergency, fire, evacuation, and disaster recovery activities. Access controls should also be tested on a no-notice basis. Tests are best scheduled or conducted early in the inspection rather than after everyone is alerted to the presence of the inspection team. Special concern, guidance, and instructions must be taken into consideration when the AIS facility has armed guards. It is possible to test the adequacy of programmed controls and data authorization by submitting jobs that attempt to bypass these controls. Take care not to destroy live data. However, if AIS upper management believes error detection and correction controls really work, then there should be no objection to the introduction of deliberate errors to test these controls.

The inspection team should convene periodically, preferably at the end of each day's activity, to review progress and to compare notes. Areas of weakness or concern should be highlighted, and additional tests or interviews scheduled to investigate further any particular areas of concern. Copies of the inspection working paper should be classified, numbered, dated, and organized for ease of understanding, review, and comparison.

At the completion of the inspection, a written report is to be prepared immediately, while impressions are still fresh. As a rule, the inspection report includes:

- An executive summary;
- A description of the inspection—dates, locations, scope, objectives, and so forth;

- A detailed report of observations made;
- Conclusions drawn from the observations; and
- Recommendations for corrective actions, as appropriate.

The degree of cooperation received should be noted and favorable conclusions should be given the same prominence as deficiencies. Tables, charts, and matrices of results, statistical tests, and conclusions may be very helpful. Distribute the final report to the AIS facility and the command upper management as prescribed in the planning phase.

INSPECTION FOLLOW-UP

An inspection is of little use unless it is the basis for improvement, correction, and management follow-up. The responsibility for implementation of such activity normally resides with the commanding officer (CO) of the command. The CO must, in turn, assign responsibilities for corrective action. The best approach is to summarize each major deficiency on a control sheet, outlining requirements, problem definition, responsibility, action taken or required, and follow-up action. In addition, an indication should be made of the date that action should be completed, or if it is to continue. Some of the corrective action may require additional funds; this should be noted.

Corrective action, follow-up, and disposition of the deficiencies should follow a recurring reporting cycle to upper management. Quarterly reports are recommended for any inspection control items still open.

The final step is a frank and honest evaluation of the inspection itself by AIS facility management and the inspection team. A group discussion should be held with the expressed purpose of improving future inspection procedures and processes. The inspection plan may need to be amended or the team composition may need to be changed. The emphasis of the inspection should always be positive—one of helping AIS management at all levels to improve the security and control of the AIS facility.

DATA PRIVACY

The Privacy Act of 1974 (Public Law 93-579) imposes numerous requirements upon naval commands to prevent the misuse or compromise of data concerning individuals. Navy AIS facilities that process personal data must provide a reasonable degree of protection against unauthorized disclosure, destruction, or

modification of personal data, whether it is intentional or results from an accident or carelessness.

Department of the Navy Information Systems Security (INFOSEC) Program, SECNAVINST 5239.3, provides guidelines for use by all Navy organizations in implementing any security safeguards that they must adopt to implement the Privacy Act. It describes risks and risk assessment, physical security measures, appropriate information management practices, and computer system/network security controls.

Department of the Navy Privacy Act (PA) Program, SECNAVINST 5211.5, implements the Privacy Act and personal privacy and rights of individuals regarding their personal records. It delineates and prescribes policies, conditions, and procedures for the following:

- Any Department of the Navy system of records possessing a record on an individual must verify it has the record upon the request of the individual.
- The identity of any individual requesting personal record information maintained on them must be confirmed before the information is released.
- An individual must be granted access to his/her personal files on request.
- Any request from an individual concerning the amendment of any record or information pertaining to the individual for the purpose of making a determination on the request or appealing an initial adverse determination must be reviewed.
- Personal information is collected, safeguarded, and maintained, and decisions are made concerning its use and dissemination.
- The disclosure of personal information, and decisions concerning which systems records are to be exempted from the Privacy Act.
- Rules of conduct are established for the guidance of Department of the Navy personnel who are subject to criminal penalties for noncompliance with the Privacy Act.

The Chief of Naval Operations is responsible for administering and supervising the execution of the Privacy Act and SECNAVINST 5211.5 within the Department of the Navy. Additionally, the Chief of Naval Operations is designated as the principal Privacy Act coordinator for the Department of the Navy.

The major provisions of the Privacy Act that most directly involve computer security are found in the following parts of title 5, United States Code (U.S.C.), section 552a:

1. Subsection (b)—limits disclosure of personal information to authorized persons and commands.
2. Subsection (e)(5)—requires accuracy, relevance, timeliness, and completeness of records.
3. Subsection (e)(10)—requires the use of safeguards to ensure the confidentiality and security of records.

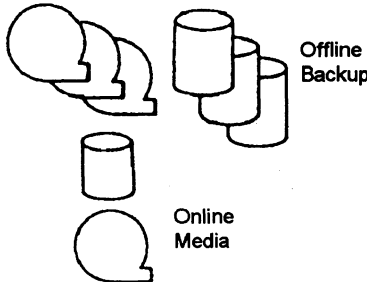
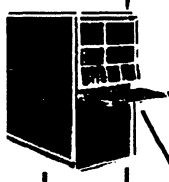
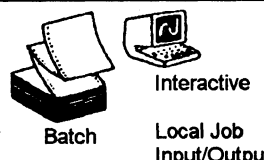


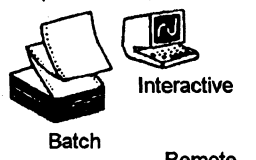
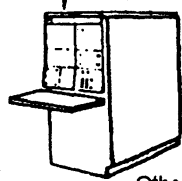
The following terminology is used in discussing the treatment of personal data:

- **Confidentiality.** A concept that applies to data. It is the status accorded to data that requires protection from unauthorized disclosure.
- **Data integrity.** The state existing when data agrees with the source from which it is derived, and when it has not been either accidentally or maliciously altered, disclosed, or destroyed.
- **Data Security.** The protection of data from accidental or intentional, but unauthorized, modification, destruction, or disclosure.

Safeguards that provide data protection are grouped into three categories: physical security measures, information management practices, and computer system/network security controls. Specifically, these are:

- **Physical security measures.** Measures for protecting the physical assets of a system and related facilities against environmental hazards or deliberate actions as discussed earlier in this chapter.
- **Information management practices.** Procedures for collecting, validating, processing, controlling, and distributing data.
- **Computer system/network security controls.** Techniques available in the hardware and software of a computer system or network for controlling the processing of and access to data and other assets.

Technological safeguards for security risks are presented in figure 4-15. They may be viewed in relation to the control points within a computer

RISKS	SYSTEM ELEMENTS	SAFEGUARDS
Erasure Theft Copying Loss Misplacement	 <p>Offline Backup</p> <p>Online Media</p>	<p>Physical Security</p> <ul style="list-style-type: none"> - Entry Controls - Storage Protection <p>Information Management Practices</p> <ul style="list-style-type: none"> - Physical Handling - Manual Access - Input Processing - Procedural Auditing <p>Systems Security</p> <ul style="list-style-type: none"> - Data Encryption for classified data
Accidental Damage Misrouting Disclosure Poor Control & Partitioning	 <p>Processors including Main Memory Aux. Memory</p>	<p>Physical Security</p> <ul style="list-style-type: none"> - Entry Controls <p>Information Management Practices</p> <ul style="list-style-type: none"> - Input Processing - Programming Practices <p>Systems Security</p> <ul style="list-style-type: none"> - Access Controls
Unauthorized Access Program Changes Eavesdropping Unauthorized Disclosures (Dumps) System Modifications	 <p>Batch</p> <p>Interactive</p> <p>Local Job Input/Output</p>	<p>Systems Security</p> <ul style="list-style-type: none"> - Identification - Access Controls - Access Auditing - Data Encryption for classified data
Misrouting Eavesdropping	 <p>Common Carrier Switching</p>	<p>Systems Security</p> <ul style="list-style-type: none"> - Data Encryption for classified data
Disclosure Misrouting	 <p>Network Interface</p>	<p>Physical Security</p> <ul style="list-style-type: none"> - Entry Controls <p>Information Management Practices</p> <ul style="list-style-type: none"> - Programming Practices <p>Systems Security</p> <ul style="list-style-type: none"> - User Authorization - Access Auditing - Data Encryption for classified data
Unauthorized User Unauthorized Terminal	 <p>Batch</p> <p>Interactive</p> <p>Remote Terminals</p>	<p>Physical Security</p> <ul style="list-style-type: none"> - Entry Controls <p>Information Management Practices</p> <ul style="list-style-type: none"> - Manual Access <p>Systems Security</p> <ul style="list-style-type: none"> - Identification - Access Controls - Data Encryption for classified data
Unauthorized Terminals Programmed Attack	 <p>Other Systems/Networks</p>	<p>Physical Security</p> <ul style="list-style-type: none"> - Entry Controls <p>Information Management Practices</p> <ul style="list-style-type: none"> - Input Processing - Programming Practices <p>Systems Security</p> <ul style="list-style-type: none"> - Identification - Access Controls

RMJA0038

Figure 4-15.—Personal data security risks and technological safeguards.

system/network. This perspective shows the elements of a computer system/network, beginning with the offline storage of personal data in machine-readable media (for example, tapes and disks) and progressing through the many possible processing modes. It includes the use of interactive computer terminals at local and remote locations and the linking of local systems via communications networks. It stresses the value of physical security measures and information management practices, in relation to computer system/network controls.

PERSONAL DATA RISK ASSESSMENT

The first step toward improving a system's security is to determine its security risks using the criteria discussed earlier in this chapter. A personal data security risk assessment benefits a command in three ways:

- It provides a basis for deciding whether additional security safeguards are needed for personal data.
- It ensures that additional security safeguards help to counter all the serious personal data security risks.
- It saves money that might have been wasted on safeguards that do not significantly lower the overall data risks and exposures.

The goal of a risk assessment is to identify and prioritize those events that would compromise the integrity and confidentiality of personal data. The seriousness of a risk depends both on the potential impact of the event and its probability of occurrence.

In general, the risk assessment should consider all risks, not just risks to personal data. While this section of the chapter emphasizes the security of personal data, it is best to develop an integrated set of security safeguards and requirements that protect all classified and other valuable data in the system wherever possible.

The risk assessment should be conducted by a team which is fully familiar with the problems that occur in the daily handling and processing of the personal information. The participants on the risk assessment team should include:

- A representative of the operating facility supported by or having jurisdiction over the data under consideration;

- The programmer responsible for support of the operation or function under consideration;
- A representative from the facility responsible for managing AIS operations;
- A system programmer (if the command has system programmers in a separate fictional area);
- A computer specialist assigned the responsibility for overseeing or inspecting system security; and
- The individual responsible for security.

PERSONAL DATA SECURITY RISKS

Each command should identify its specific risks and evaluate the impact of those risks in terms of its information files. Experience indicates the most commonly encountered security risks are usually accidents, errors, and omissions. The damage from these accidental events far exceeds the damage from all other personal data security risks. Good information management practices are necessary to reduce the damage that can result from these occurrences. Personal data security risks include:

- **Input error.** Data may not be checked for consistency and reasonableness at the time they are entered into the system; or data may be disclosed, modified, lost, or misidentified during input processing.
- **Program errors.** Programs can contain many undetected errors, especially if they were written using poor programming practices or were not extensively tested. A program error may result in undesirable modification, disclosure, or destruction of sensitive information.
- **Mistaken processing of data.** Processing requests may update the wrong data; for example, a tape mounted at the wrong time.
- **Data loss.** Personal data on paper printouts, magnetic tapes, or other removable storage media may be lost, misplaced, or destroyed.
- **Improper data dissemination.** Disseminated data may be misrouted or mislabeled, or it may contain unexpected personal information.
- **Careless disposal of data.** Personal data can be retrieved from wastepaper baskets, magnetic tapes, or discarded files.

Every AIS facility's technical manager and upper management should establish strict controls and procedures over individuals authorized to access the personal data files. If everyone at the facility needs authority to access personal data files, the security measures should adequately control system access. If there are persons working on the system whose access should be limited, the following risks should be considered:

- **Open system access.** This means there may be no control over who can either use the AIS or enter the computer room.
- **Theft of data.** Personal data may be stolen from the computer room or other places where it is stored.
- **Unprotected files.** Personal data files may not be protected from unauthorized access by other users of the AIS. This applies to online files and also to offline files, such as files on magnetic tapes. The offline files are sometimes accessible simply by requesting a tape be mounted.
- **Dial-in access.** There is serious danger that unauthorized persons can access the system when remote, dial-in access is allowed.
- **Open access during abnormal circumstances.** Personal data that is adequately protected during normal operations may not be adequately protected under abnormal circumstances. Abnormal circumstances include power failures, bomb threats, and natural disasters, such as fire or flood.

The physical destruction or disabling of the AIS is not normally a primary risk to privacy. However, all computer systems presently in use are vulnerable to deliberate penetrations that can bypass security controls. These types of security penetrations require extensive technical knowledge. At present, the Navy has experienced very few of these deliberate penetrations. Commands designing large computer networks should consider the following risks early in the planning stage:

- **Misidentified access.** Passwords are often used to control access to a computer or to data, but they are notoriously easy to obtain if their use is not carefully controlled. Furthermore, a person may use an already logged-in terminal, which the authorized user has left unattended, or may capture a communications port as an authorized user attempts to disconnect from it.

- **Operating system flaws.** Design and implementation errors in operating systems allow a user to gain control of the system. Once the user is in control, the auditing controls can be disabled, the audit trails erased, and any information on the system accessed.
- **Subverting programs.** Programs containing hidden subprograms that disable security protections can be submitted. Other programs can copy personal files into existing or misidentified files to use when protection is relaxed.
- **Spoofing.** Actions can be taken to mislead system personnel or the system software into performing an operation that appears normal but actually results in unauthorized access.
- **Eavesdropping.** Communications lines can be monitored by unauthorized terminals to obtain or modify information or to gain unauthorized access to an AIS.

INFORMATION MANAGEMENT PRACTICES

Information management practices refer to the techniques and procedures used to control the many operations performed on information to accomplish the command's objectives. They do not extend to the essential managerial determination of the need for and uses of information in relation to any command's mission. In this context, information management includes data collection, validation and transformation; information processing or handling; record keeping; information control, display, and presentation; and, finally, standardization of information management operations.

Before enacting new policies in personal data handling procedures, AIS technical managers should analyze current practices. To facilitate the explanation of their roles, the information management guidelines presented in the following material are grouped into major categories: handling of personal data, maintenance of records to trace the disposition of personal data, data processing practices, programming practices, assignment of responsibilities, and procedural inspecting. Every practice presented may not be required at every Navy AIS facility by upper management. Select only the suggested practices relevant to the designated command's environment and mission, or approved by upper management.

Handling of Personal Data

Access to personal information will be limited to authorized individuals of agencies in the Department of Defense who have an official need for the record, except when the information is otherwise releasable under the disclosure or access provisions of the Privacy Act.

The following practices are suggested for the handling of personal data:

- Prepare a procedures handbook. Describe the precautions to be used and obligations of computer facility personnel during the physical handling of all personal data. Include a reference regarding the applicability of the procedures to those government contractors who are subject to the Privacy Act. Personal information that is processed, accessed, maintained, or disposed of by contractors must be handled within the terms and conditions of Section 7-104.96 of the Defense Acquisition Regulation.
- Label all recording media that contain personal data. Labeling the media reduces the probability of accidental abuse of personal data. It also aids in fixing the blame in the event of negligent or willfully malicious abuse. If the information resides on removable storage media, it should be externally labeled. External warnings must clearly indicate that the media contain personal information subject to the Privacy Act; for example, PERSONAL DATA—PRIVACY ACT of 1974. Note that abbreviations must not be used.
- Store personal data in a manner that conditions users to respect its confidentiality. For example, store personal data under lock and key when not being used.
- If a program generates reports containing personal data, have the program print clear warnings of the presence of such data on the reports.
- Color code all computer tape reels, disk pack covers, and so on, which contain personal data, so they can be afforded the special protection required by law.
- Keep a record of all categories of personal data contained in computer-generated reports. This facilitates compliance with the requirements that each command identify all personal data files and their routine uses by the command.

- Carefully control products of intermediate processing steps. For example, control scratch tapes and disk packs to ensure they do not contribute to unauthorized disclosure of personal data.
- Maintain an up-to-date hard-copy authorization list. The list should include all individuals (computer personnel as well as system users) allowed to access personal data. It is used in access control and authorization validation.
- Maintain an up-to-date hard-copy data dictionary. This dictionary should be the complete inventory of personal data files within the computer facility to account for all obligations and risks.

Maintenance of Records to Trace the Disposition of Personal Data

The following practices are suggested for the maintenance of records:

- Establish procedures for maintaining correct, current accounting of all new personal data brought into the computer facility.
- Log each transfer of storage media containing personal data to or from the computer facility.
- Maintain logbooks for terminals used to access personal data by system users.

Data Processing Practices

The following practices are suggested for data processing procedures:

- Use control numbers to account for personal data upon receipt and during input, storage, and processing.
- Verify the accuracy of the personal data acquisition and entry methods employed.
- Take both regular and unscheduled inventories of all tape and disk storage media to ensure accurate accounting for all personal data.
- Use carefully devised backup procedures for personal data. A copy of the data should be kept at a second location if its maintenance is required by law.
- Create a records retention timetable covering all personal data and stating minimally the data

type, the retention period, and the authority responsible for making the retention decision.

- After a computer failure, check all personal data that was being processed at the time of failure for inaccuracies resulting from the failure.
- If the data volumes permit economic processing, some sensitive applications may use a dedicated processing period.
- Examine files created from files known to contain personal data to ensure they cannot be used to regenerate any personal data. A formal process must be established to determine and certify that such files are releasable in any given instance.
- In aggregating personal data, consider whether the consequent file has been increased in value to a theft-attracting level.
- When manipulating aggregations and combinations of personal data, make it impossible to trace any information concerning an individual. Take steps so that no inference, deduction, or derivation processes can be used to recover personal data.

Programming Practices

The following practices are suggested for programming procedures:

- Subject all programming development and modification to independent checking by a second programmer, bound by procedural requirements developed by a responsible supervisor.
- Inventory current programs that process or access personal data; verify their authorized usage.
- Enforce programming practices that clearly and fully identify personal data in any computer program.
- Strictly control and require written authorization for all operating system changes that involve software security.

Assignment of Responsibilities

The following practices are suggested for the assignment of responsibilities:

- Designate an individual responsible for examining facility practices in the storage, use, and processing of personal data, including the use of security measures, information management practices, and computer system access controls. Both internal uses and the authorized external transfer of data should be considered by this individual and any risks reported to the relevant upper management authority and the AIS technical manager.
- Designate an individual responsible during each processing period (shift) for ensuring the facility is adequately staffed with competent personnel and enforcing the policies for the protection of personal data.
- Ensure that all military, civil service, and other employees engaged in the handling or processing of personal data adhere to established codes of conduct.

Procedural Inspecting

Whenever appropriate, conduct an independent examination of established procedures. Inspections of both specific information flow and general practices are possible. The following points should be considered when developing an inspection:

- Inspecting groups can be established within organizations to provide assurance of compliance independent of those directly responsible.
- Independent, outside inspectors can be contacted to provide similar assurance at irregular intervals.
- Inspection reports should be maintained for routine inspection and used to provide additional data for tracing compromises of confidentiality.

IDENTIFICATION TECHNIQUES

Once security measures and information management practices are established, the AIS technical manager should consider methods of personal identification of individuals for authorized access to the AIS facility. The identification of each individual allowed to use a system is a necessary step in safeguarding the data contained in that system.

For a broader knowledge of personal identification and identification techniques, refer to *Guidelines on*

SUMMARY

AIS security is everyone's job. The key word is *PROTECT*: take all reasonable measures to protect our AIS assets. Be sure you know what to do if a fire breaks out, the air conditioning goes off, the power goes down (with or without an UPS), or an unauthorized person is in your computer facility.

Learn the AIS terminology and requirements. Keep alert; early detection of problems is the key to minimizing damage and destruction.

Security of all types should be a continuous matter with every AIS technical manager. In this chapter, we have scratched only the surface of the material available on classified security, physical security, and security and privacy of data. It is a subject with which everyone should be completely up-to-date. Study the material presented and referenced in this chapter to become knowledgeable in AIS security.